US006121962A

United States Patent [19]

Hwang

[11] **Patent Number: 6,121,962**

[45] **Date of Patent: Sep. 19, 2000**

[54] **COMPUTER SYSTEM AND METHOD FOR CONTROLLING SCREEN DISPLAY OF A MONITOR IN A POWER MANAGEMENT MODE**

[75] Inventor: **Hae-Jin Hwang**, Suwon, Rep. of Korea

[73] Assignee: **SamSung Electronics Co., Ltd.**, Kyungki-do, Rep. of Korea

[21] Appl. No.: **09/075,318**

[22] Filed: **May 11, 1998**

[30] **Foreign Application Priority Data**

Jun. 16, 1997 [KR] Rep. of Korea 97-24852

[51] **Int. Cl.^{7}** **G09G 65/00**

[52] **U.S. Cl.** **345/211**; 345/204; 713/202; 713/300

[58] **Field of Search** 345/204, 211–214, 345/210; 713/202, 300, 324, 323

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,752,044 5/1998 Crump et al. 395/750.05
5,875,345 2/1999 Naito et al. 395/750.05
5,931,948 8/1999 Morisawa et al. 713/202

Primary Examiner—Amare Mengistu
Assistant Examiner—Mansour M. Said
Attorney, Agent, or Firm—Robert E. Bushnell, Esq.

[57] **ABSTRACT**

A computer system for controlling a screen display state of a monitor according to input of a password for protecting confidential information from unauthorized users when a computer system is between a standby mode and a suspend mode. The computer system comprises a power controller for converting an operation mode of a computer system into a power management mode which represents one of a power-on mode, a standby mode, a graphic off mode, and a suspend mode according to an access state of the computer system; and a screen controller for converting a screen display state of the display according to a designated one of the power management mode, and controlling the screen display state of the monitor according to input of a password if the computer system is accessed in the graphic off mode.

13 Claims, 5 Drawing Sheets

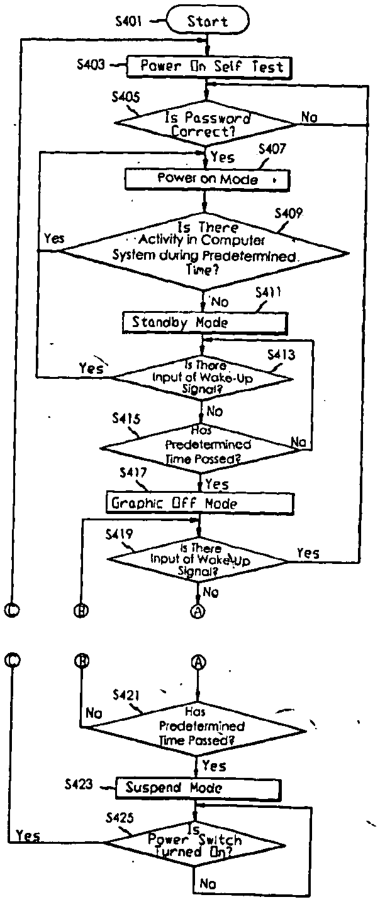

S401
Start
S403
Power On Self Test
S405
Is Password Correct?
No
Yes
S407
Power on Mode
S409
Is There Activity in Computer System during Predetermined Time?
Yes
No
S411
Standby Mode
S413
Is There Input of Wake-Up Signal?
Yes
No
S415
Has Predetermined Time Passed?
No
Yes
S417
Graphic Off Mode
S419
Is There Input of Wake-Up Signal?
Yes
No
C
B
A
C
B
A
S421
Has Predetermined Time Passed?
No
Yes
S423
Suspend Mode
S425
Is Power Switch Turned On?
Yes
No

FIG. 1

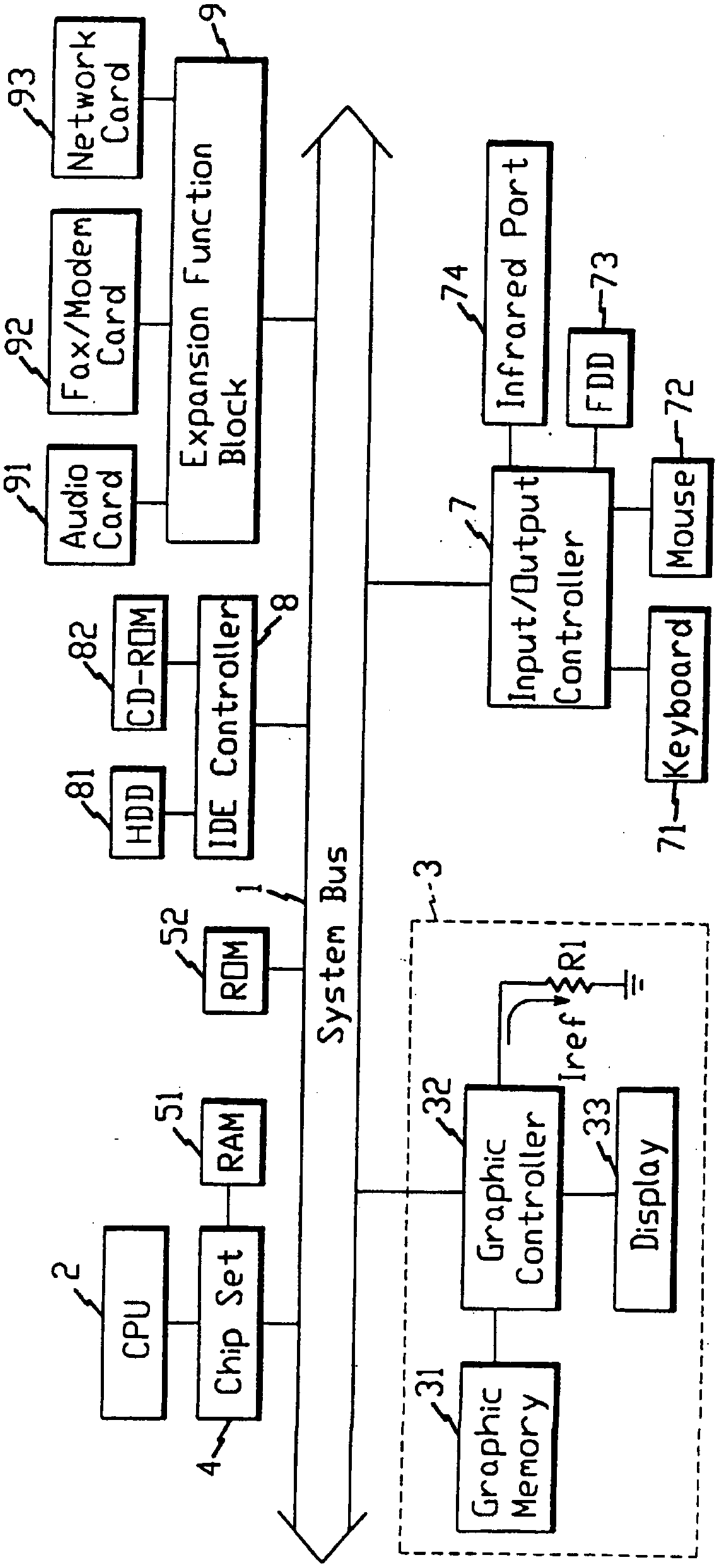

CPU
2
Chip Set
4
RAM
51
ROM
52
System Bus
1
IDE Controller
8
HDD
81
CD-ROM
82
Expansion Function Block
9
Audio Card
91
Fax/Modem Card
92
Network Card
93
Infrared Port
74
FDD
73
Input/Output Controller
7
Mouse
72
Keyboard
71
3
Graphic Memory
31
Graphic Controller
32
Display
33
Iref
R1

FIG. 2

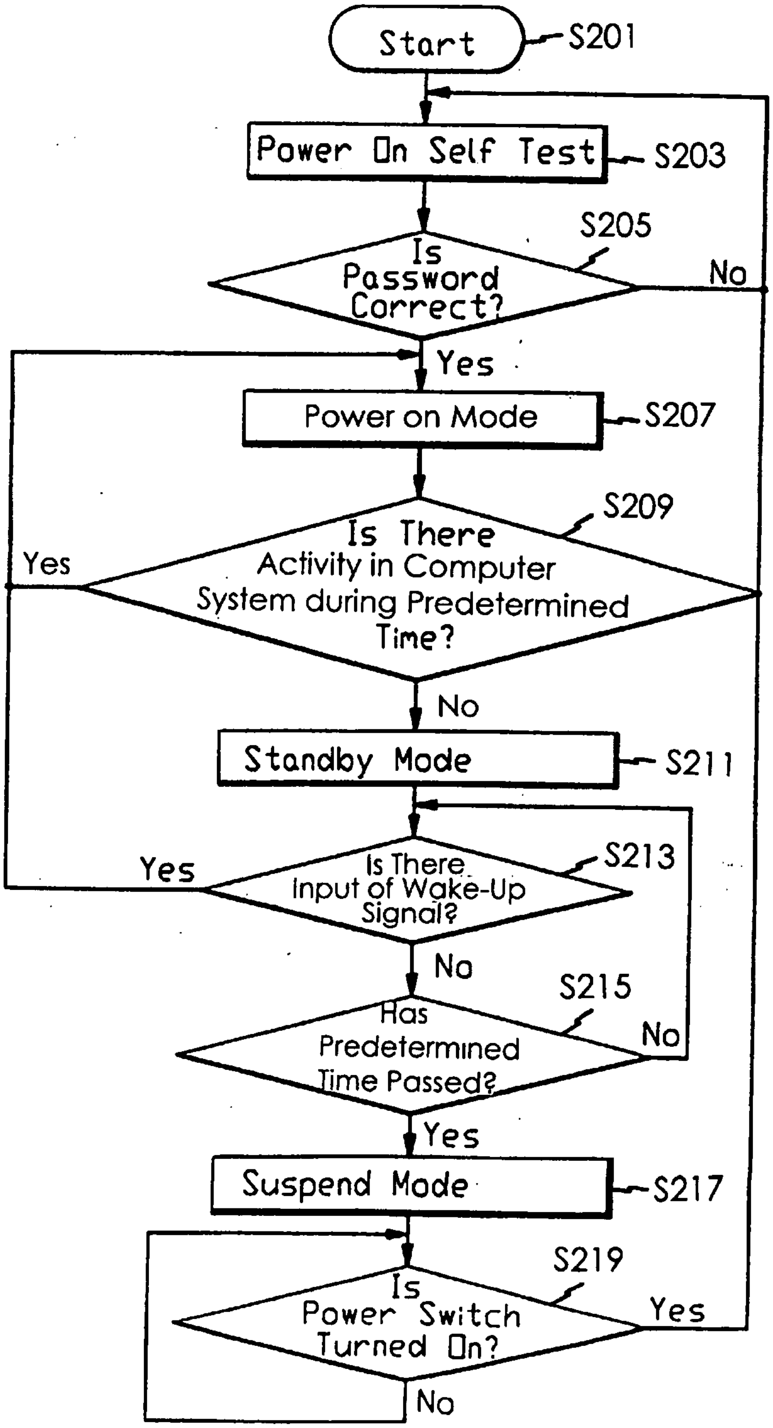

Start
S201
Power On Self Test
S203
S205
Is Password Correct?
No
Yes
Power on Mode
S207
S209
Is There Activity in Computer System during Predetermined Time?
Yes
No
Standby Mode
S211
S213
Is There Input of Wake-Up Signal?
Yes
No
S215
Has Predetermined Time Passed?
No
Yes
Suspend Mode
S217
S219
Is Power Switch Turned On?
Yes
No

FIG. 3

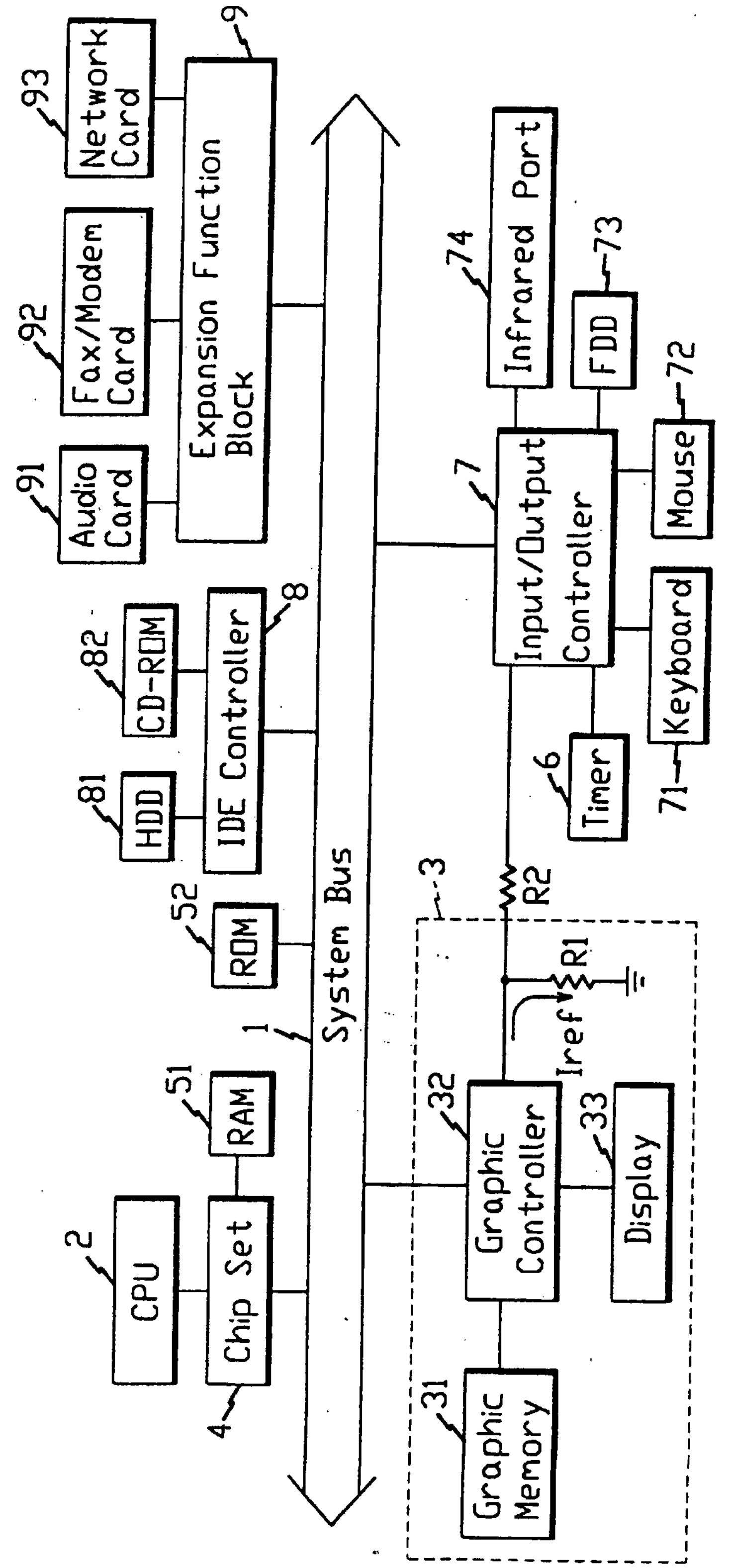

CPU
2
Chip Set
4
RAM
51
ROM
52
System Bus
1
HDD
81
CD-ROM
82
IDE Controller
8
Audio Card
91
Fax/Modem Card
92
Network Card
93
Expansion Function Block
9
Input/Output Controller
7
Infrared Port
74
FDD
73
Mouse
72
Keyboard
71
Timer
6
R2
R1
Iref
3
Graphic Controller
32
Display
33
Graphic Memory
31

FIG. 4A

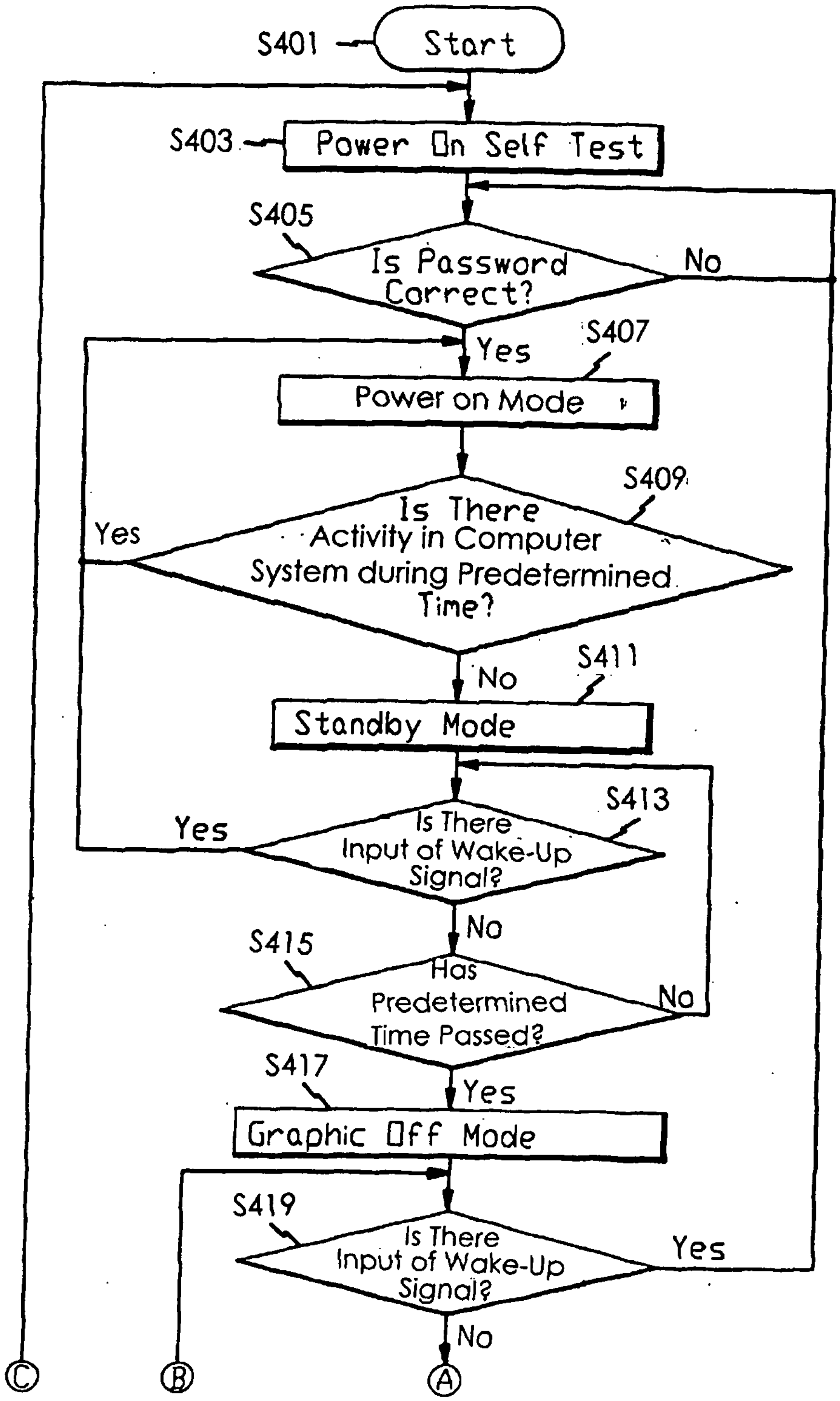
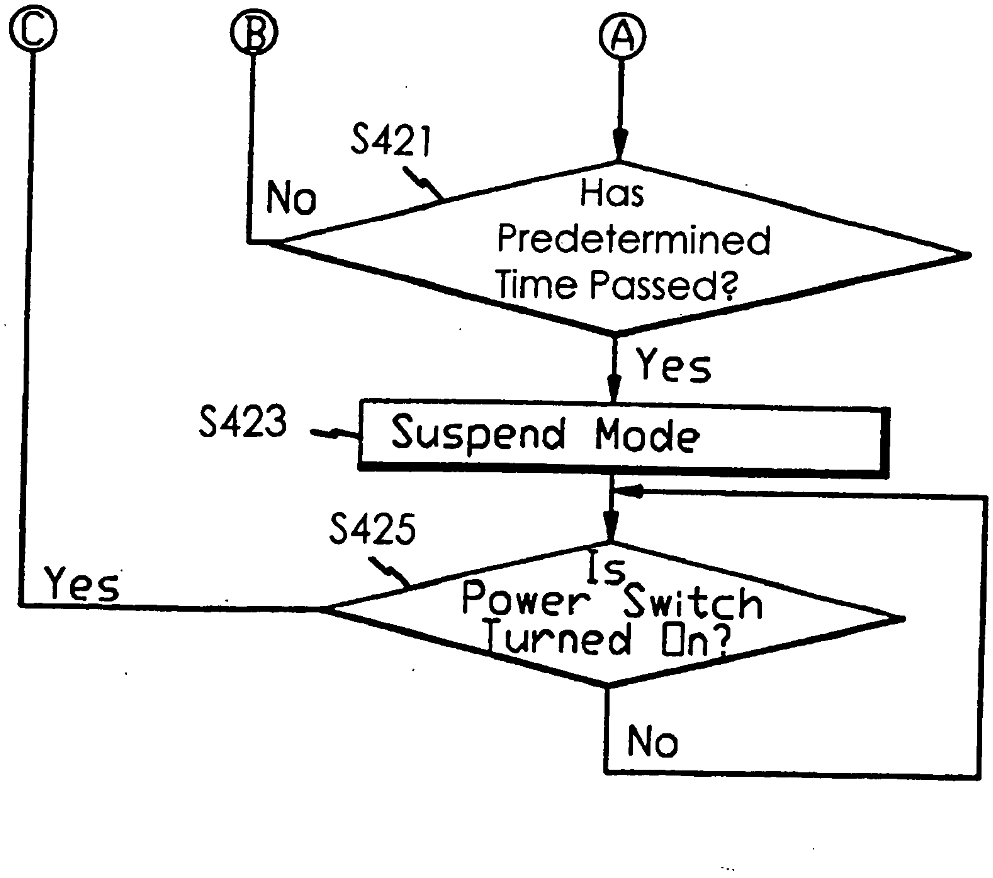

S401
Start
S403
Power On Self Test
S405
Is Password Correct?
No
Yes
S407
Power on Mode
S409
Is There Activity in Computer System during Predetermined Time?
Yes
No
S411
Standby Mode
S413
Is There Input of Wake-Up Signal?
Yes
No
S415
Has Predetermined Time Passed?
No
Yes
S417
Graphic Off Mode
S419
Is There Input of Wake-Up Signal?
Yes
No
C
B
A

FIG. 4B


C
B
A
S421
No
Has Predetermined Time Passed?
Yes
S423
Suspend Mode
S425
Yes
Is Power Switch Turned On?
No

COMPUTER SYSTEM AND METHOD FOR CONTROLLING SCREEN DISPLAY OF A MONITOR IN A POWER MANAGEMENT MODE

CLAIM FOR PRIORITY

This application makes reference to, incorporates the same herein, and claims all benefits accruing under 35 U.S.C. §119 from an application for COMPUTER SYSTEM BEING CAPABLE OF CONTROLLING SCREEN DISPLAY STATE AND METHOD THEREOF earlier filed in the Korean Industrial Property Office on the of Jun. 16th 1997, and there duly assigned Ser. No. 24852/1997, a copy of which application is annexed hereto.

BACKGROUND OF THE INVENTION

1. Technical Field

The present invention relates to a computer system for controlling a screen display of a monitor in a power management mode, and more particularly, relates to a computer system for controlling a screen display of a monitor in a power management mode according to input of a password for protecting confidential information from unauthorized users when the computer system is reawakened from a graphic off mode.

2. Related Art

Contemporary computer systems generally consist of a main unit (which may have built-in storage devices such as floppy disks, hard disks and CD-ROM), a keyboard and a monitor. The main unit may be connected to a cathode-ray tube (CRT) monitor and other peripheral devices. In normal usage, it is common for the monitor and other peripherals to be turned on and to remain on for as long as the computer is running, even though the peripherals are actually used only a small percentage of the time. A typical color video monitor, for example, may consume as such as 50 to 80 percent of the total electrical energy consumed by a personal computer (PC). If the monitor consumes valuable energy only to remain idle, not only the valuable energy resources will be wasted but the life of the monitor will decrease rapidly. Obviously, power can be conserved if the user turns the computer system off or in a standby mode each time the computer system is no longer in use for a prolonged period. This requirement is, however, impractical. Therefore, system should be designed to automatically conserve valuable energy resources when the computer system is not in use.

In principle, automatically saving energy by turning off the computer system is fairly easy. Computer systems are invariably designed so that if there is no activity from the keyboard or from other external inputs during a specified time, the computer systems are turned off or placed in a standby mode to save energy. Only minimal logic is kept active to detect when the keyboard or other external inputs are becoming active again so as to turn the computer system back on. Conventional power saving features for typical personal computers having monitors as separate items are disclosed, for example, in U.S. Pat. No. 5,163,124 for Method And Apparatus For Controlling Power To Device In A Computer System issued to Yabe et al., U.S. Pat. No. 5,218,704 for Real Time Power Conservation For Portable Computers issued to Watts, Jr., U.S. Pat. No. 5,375,245 for Apparatus For Automatically Reducing The Power Consumption Of A CRT Computer Monitor issued to Solhjell et al., U.S. Pat. No. 5,389,952 for Low-Power-Consumption Monitor Standby System issued to Kikinis, U.S. Pat. No. 5,408,668 for Method And Apparatus For Controlling The Provision Of Power To Computer Peripherals issued to Tornai, U.S. Pat. No. 5,410,713 for Power Management System For A Computer issued to White, and recently U.S. Pat. No. 5,483,464 for Power Saving Apparatus For Use In Peripheral Equipment Of A Computer issued to Song and assigned to the same assignee of the present invention. Usually, the monitor is shut down during the period of inactivity with the exception of a small amount of power necessary to detect when the computer system becomes active again so as to resume operation of the monitor. Generally, when the monitor is powered normally, the display of data image is blanked during the period of inactivity and re-displayed when the computer system becomes active, i.e., when an input device such as a keyboard is operated. During this type of blanking, however, the monitor continues to consume normal power.

Display power management standards have been set to save power consumption by controlling monitor power with respect to the operational status of the computer system. In the power management mode, power supply is managed according to the operational status of the computer system. The mode status of the power management is classified into power-on, standby, suspend and power-off. First, when the computer system is first turned on, power is continuously supplied to each device of the computer system in a power-on mode. After a period of inactivity, the computer system is switched to a standby mode to reduce power consumption by lowering the operation frequency of a central processing unit (CPU), turning off operation of a monitor, and turning off operation of a hard disk drive (HDD). The computer system may also be temporarily suspended in a suspend mode when there is a sudden power failure or when the computer system is not accessed for a predetermined time period. Lastly, the computer system may be turned off completely in a power-off mode.

During the standby mode, the computer system can be automatically awakened and the mode of the computer system is converted back into the full power-on mode without checking a password when there is an external input such as input from a keyboard, a mouse, and an infrared port, and activity from a hard disk drive (HDD), a floppy disk drive (FDD), a fax/modem card, and a network card. During the suspend mode, the computer system provides a visual display of identification information such as "enter password" on a monitor when the power switch is turned on if the password is set at the time of the computer setup, and the mode of the computer system is converted into the full power-on mode after checking that the input password is correct. The mode of the computer system is converted into the full power-on mode without checking the password if the password is not set at the time of the computer setup.

The mode of the computer system is converted into the full power-on mode after checking the password if the password is set at the time of the computer setup when the power switch is turned on, and the mode of the computer system is converted back into the full power-on mode without checking the password if the password is not set at the time of the computer setup. However, typical computer system, as I have observed, has a disadvantage in that information can not be kept confidential from unauthorized users since the password is not needed, before the computer system is converted into a suspend mode, to convert the computer system back into a full power-on mode.

SUMMARY OF THE INVENTION

Accordingly, it is therefore an object of the present invention to provide a computer system for controlling a screen display of a monitor in a power management mode.

It is also an object to provide a computer system for protecting confidential information from unauthorized users when a monitor is reawaken from a standby mode.

It is another object to provide a computer system for operating in a graphic off mode to turn off a screen display of a monitor for protection against unauthorized users after the monitor is in a standby mode for a predetermined time period.

It is further an object to provide a computer system for requesting input of a correct password while operating in a graphic off mode before returning to a full power-on mode.

These and other objects of the present invention can be achieved by a computer system having a central processing unit, a memory, a system bus and a monitor and comprises a power controller for converting an operation mode of a computer system into a power management mode representing one of a power-on mode, a standby mode, a graphic-off mode, and a suspend mode according to an access state of the computer system; and a screen controller for converting a screen display state of a monitor according to a designated one of the specific power management mode, and for controlling the screen display state of the monitor according to input of a password when the computer system is accessed in the graphic off mode.

According to another aspect of the present invention, a method for controlling a screen display state of a computer system, comprises the steps of: converting the mode of a computer system into a standby mode if power is applied to the computer system and there is no access to the computer system; converting a screen display state of a monitor if there is no access to the computer system for a predetermined time in a standby mode, and converting the mode of the computer system to a graphic off mode in which the screen output state of the monitor is controlled according to input of a password if the computer system is again accessed; and controlling the power supply provided to the computer system according to the operation of a power switch by converting the mode of the computer system into the suspend mode if the computer system is not accessed for the predetermined time in the graphic off mode.

The present invention is more specifically described in the following paragraphs by reference to the drawings attached only by way of example.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of the present invention, and many of the attendant advantages thereof, will become readily apparent as the same becomes better understood by reference to the following detailed description when considered in conjunction with the accompanying drawings in which like reference symbols indicate the same or similar components, wherein:

FIG. 1 is a block diagram of a typical computer system for controlling a screen display of a monitor in a power management mode;

FIG. 2 illustrates a flow chart of a process of controlling a screen display of a monitor in a power management mode;

FIG. 3 is a block diagram of a computer system for controlling a screen display of a monitor in a power management mode according to the principles of the present invention; and

FIGS. 4A and 4B illustrate a flow chart of a process of controlling a screen display of a monitor in a power management mode according to the principles of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring now to the drawings and particularly to FIG. 1, which illustrates a computer system for controlling a screen display of a monitor in a power management mode. As shown in FIG. 1, the computer system includes a system bus 1, a central processing unit (CPU) 2, a display device 3 such as a CRT monitor, a chip set 4, an input/output controller 7, an integrated device electronics (IDE) controller 8, an expansion function block 9, a random-access-memory (RAM) 51, a read-only-memory (ROM) 52, a keyboard 71, a mouse 72, a floppy disk drive (FDD) 73, an infrared port 74, a hard disk drive (HDD) 81, a compact disk read-only-memory (CD-ROM) 82, an audio card 91, a fax/modem card 92, and a network card 93.

The system bus 1, is an input/output interface applied to a micro-processor, for connecting data, command, and interrupt in the computer system to each circuit block or each device. The CPU 2 is connected to the system bus 1 for controlling the computer system. The monitor 3 provides visual display of information data on a screen. The chip set 4 is connected to the system bus 1 for converting the mode of the computer system into a specific power management mode by controlling video signals output from the monitor 3, the operation frequency of the CPU 2 and the operation state of the HDD 81 according to the access state to the computer system. The RAM 51 is connected to the chip set 4 and serves as a memory area where the CPU 2 stores a system software and a user software.

The input/output controller 7 is connected to the system bus 1 for controlling the input or output from the keyboard 71, the mouse 72, the infrared port 74 and the FDD 73. The IDE controller 8 is connected to the HDD 81 and the CD-ROM 82 via the system bus 1 for controlling the input or output of the HDD 81 and the CD-ROM 82. The ROM 52 is connected to the system bus 1 and stores specific application programs that are used by the CPU 2. The expansion function block 9 supports the audio card 91, the fax/modem card 92 and the network card 93 for function expansions in the computer system.

The monitor 3 includes a graphic memory 31 for storing data to be displayed on the screen; a graphic controller 32 for reading the data from the graphic memory 31 and converting the data into R,G,B signals; a first resistor R1 having one terminal connected to the graphic controller 32 and the other terminal grounded in order to control the brightness of the R,G,B signals; and a display unit 33 for receiving the R,G,B signals output from the graphic controller 32 and providing a visual display of data information on the screen.

FIG. 2 illustrates a process of controlling a screen display of the computer system in a power management mode. First, the CPU 2 performs a POST (power on self test) procedure for checking whether the hardware operates normally, using a BIOS boot program when the power switch is turned ON and power is applied to the computer system at steps 201 and 203.

After the POST procedure is completed, the power management mode is set, and the computer system is booted by an operating system. A sentence such as "enter password" is displayed on a screen of the monitor 3 when the power switch is turned ON if the password is set at the time of the computer setup. The booting operation is completed only when the input password is correct, and the user may use the computer system. However, the user can still use the computer system since the booting operation may be completed without checking the password if the password is not set at the time of the computer setup at step 205.

In this situation, the graphic controller 32 of the monitor 3 reads data information to be displayed on the screen from the graphic memory 31, converts the data information into analog R,G,B signals and outputs the R,G,B signals. The display unit 33 receives the R,G,B signals and displays the letters or the image information on the screen if the user uses the computer system through input of the keyboard 71, the mouse 72, the infrared port 74, the access of the FDD 73, the access of the HDD 81, the access of the compact disk ROM 82, the access of the fax/modem card 92 or the access of the network card 93. Reference current Iref determines the brightness of the R,G,B signals from the graphic controller 32, and the reference current Iref is determined by the first resistor R1.

After the POST procedure is completed, the power management mode converts to the full power-on mode at step 207. The chip set 4 next converts the mode of the computer system into a standby mode by lowering the operation frequency of the CPU 2, turning OFF the R,G,B signals output from the graphic controller 32, and turning OFF the HDD 81 at step 211 if there is no input from any one of the keyboard 71, the mouse 72, the infrared port 74 via the input/output controller 7, access of the FDD 73 via the input/output controller 7, access of the HDD 81 and the CD-ROM 82 via the IDE controller 8, access of the fax/modem card 92 and the network card 93 via the expansion function block 9 for a predetermined time set for converting the full on mode into the standby mode at step 209.

The chip set 4 converts the mode of the computer system into the full power-on mode if there is input of a wake-up signal from the input/output controller 7, the IDE controller 8 and the expansion function block 9 to the CPU 2 from the keyboard 71, the input from the mouse 72, the input from the infrared port 74, the access of the FDD 73, the access of the HDD 81, the access of the CD-ROM 82, the access of the fax/modem card 92 or the access of the network card 93 at step 213. If there is no input of a wake-up signal from either the keyboard 71, the mouse 72, or the infrared port 74, access of the FDD 73, access of the HDD 81, access of the CD-ROM 82, access of the fax/modem card 92 or access of the network card 93 at step 213, the chip set 4 checks the time when the computer system operates in the standby mode and determines whether a predetermined time has passed at step 215.

When a predetermined time has passed and there is no input of a wake-up signal, the mode of the computer system is converted into a suspend mode from a standby mode at step 217. The chip set 4 senses the state of the power switch if the mode of the computer system is converted into the suspend mode. The process routine jumps to the step for performing the POST procedure if the power switch is turned ON, whereby the computer system is booted again. If the power switch is not turned ON, the power OFF state is maintained at step 219.

As I have observed however, the typical computer system has a disadvantage in that data information can not be kept confidential from unauthorized users since a password is not needed, before a computer system is converted into a suspend mode, to convert a computer system into a full power-on mode.

Turning now to FIG. 3, FIG. 3 which illustrates a computer system for controlling a screen display of a monitor in a power management mode according to the principles of the present invention. The computer system includes a system bus 1, a central processing unit (CPU) 2, a display device 3 such as a CRT monitor, a chip set 4, a timer 6, an

input/output controller 7, an integrated device electronics (IDE) controller 8, an expansion function block 9, a random-access-memory (RAM) 51, a read-only-memory (ROM) 52, a keyboard 71, a mouse 72, a floppy disk drive (FDD) 73, an infrared port 74, a hard disk drive (HDD) 81, a compact disk read-only-memory (CD-ROM) 82, an audio card 91, a fax/modem card 92, and a network card 93.

The monitor or display 3 includes a graphic memory 31, a graphic controller 32, a first resistor R1 and a display unit 33. The chip set 4 is connected to the system bus 1 for converting the mode of a computer system into a power management mode according to the operation state of the computer system by controlling R,G,B signals from the display 3, operation frequency of the CPU 2 and the operation of the HDD 81. The timer 6 is connected to the input/output controller 7 for measuring a standby mode operation time if the computer system operates in a standby mode for a predetermined time, and outputting a graphic off signal. The input/output controller 7 is, in turn, connected to the system bus 1 for converting the mode of the computer system into a graphic off mode by outputting a graphic cut-off signal if the graphic off signal is input from the timer 6, checking a password if there is an input signal from a keyboard 71, a mouse 72 or an infrared port 74, and converting the mode of the computer system into a mode in which the user can see a screen of display unit 33; of the display or monitor 3 by stopping the output of the graphic cut-off signal if the password is correct. The second resistor R2 has one terminal connected to a node between the first resistor R1 in the display 3 and the graphic controller 32, and the other terminal connected as the input/output controller 7.

The system bus 1, the CPU 2, the display 3, the RAM 51, the ROM 52, the IDE controller 8 and the expansion function block 9 of the present invention have the same function as the typical computer system as shown in FIG. 1.

Now, the operation of the computer system for controlling a screen display state according to the preferred embodiment of the present invention will be described in detail with reference to FIGS. 3 and 4A–4B hereinbelow.

First, the CPU 2 performs a POST (power on self test) procedure for checking whether the hardware operates normally, using a BIOS boot program when the power switch is turned ON and power is applied to the computer system at steps 401 and 403.

After the POST procedure is completed, the power management mode is set, and the computer system is booted by an operating system. A sentence such as "enter password" is displayed on a screen of the monitor 3 when the power switch is turned ON if the password is set at the time of the computer setup. The booting operation is completed only when the input password is correct, and the user may use the computer system. However, the user can still use the computer system since the booting operation may be completed without checking the password if the password is not set at the time of the computer setup at step 405.

Here, the graphic controller 32 in the monitor 3 reads information data to be displayed on the screen from the graphic memory 31, converts the information data into analog R,G,B signals and outputs the R,G,B signals to the display or display unit 33 if the user uses the computer system through the keyboard 71, the mouse 72, the infrared port 74, the access of the FDD 73, the access of the HDD 81, the access of the CD-ROM 82, the access of the fax/modem card 92 or the access of the network card 93. The display unit 33 receives the R,G,B signals and displays the letters or the image information on the screen of display unit 33.

Reference current Iref determines the brightness of the R,G,B signals from the graphic controller 32, and the reference current Iref is determined by the first resistor R1. The greater the first resistor R1, the lesser the reference current Iref, whereby the screen becomes dark. Generally, the value of the reference current Iref is about 3.05 mA since voltage value of the R,G,B signals from the graphic controller 32 is about 1.1V and the first resistor has a resistance value of 360 Ohm. The power management mode converts to the full power-on mode in which power is normally supplied to each part of the computer system if the computer system is used as described at step **407**.

The chip set **4** converts the mode of the computer system into the standby mode by lowering the operation frequency of the CPU **2**, turning OFF the R,G,B signals from the graphic controller **32**, and turning OFF the HDD **82** at step **411** if there is no input from any one of the keyboard **71**, the mouse **72**, and the infrared port **74** via the input/output controller **7**, access of the FDD **73** via the input/output controller **7**, access of the HDD **81** and the CD-ROM **82** via the IDE controller **8**, access of the fax/modem card **92** and the network card **93** via the expansion function block **9** for a predetermined time set for converting the full power-on mode into the standby mode at step **409**.

The R,G,B signals are turned OFF if the chip set **4** sets an R,G,B output registered in the graphic controller **32** to an OFF state, and the R,G,B signals are turned ON if the chip set **4** sets the R,G,B output register to an ON state, whereby the R,G,B signals are output to the display unit **33** for a visual display.

The timer **6** starts operating if the mode of the computer system is converted into the standby mode. The timer **6** measures the standby operation time if the computer system operates in the standby mode for a predetermined time, and outputs the graphic off signal to the input/output controller **7**. If there is input of a wake-up signal from the input/output controller **7**, the IDE controller **8** and the expansion function block **9** to the CPU **2** by any one of the keyboard **71**, the mouse **72**, the infrared port **74**, the FDD **73**, the HDD **81**, the CD-ROM **82**, the fax/modem card **92** or the network card **93** at step **413**, the chip set **4** senses the wake-up signal and converts the mode of the computer system into the full power-on mode.

However, the input/output controller **7** receives the graphic off signal and outputs the graphic cut-off signal if there is no input by the keyboard **71**, input by the mouse **72**, input by the infrared port **74**, access of the FDD **73**, access of the HDD **81**, access of the compact disk ROM **82**, access of the fax/modem card **92** or access of the network card **93** at step **413**, and the graphic off signal is outputted from the timer **6** at step **415**.

The graphic cut-off signal outputted from the input/output controller **7** is applied to the first resistor R1 in the display **3**. Here, the graphic cut-off signal has the higher voltage than the voltage of the R,G,B signals outputted from the graphic controller **32**, and prevents the reference current Iref from flowing. Accordingly, the R,G,B signals outputted from the graphic controller **32** are not output to the display unit **33**, whereby the user can not see the screen, that is, the mode of the computer system becomes the graphic off mode. The second resistor R2 is for protecting the graphic controller **32** from the graphic cut-off signal.

The chip set **4** restores the operation frequency of the CPU **2** to the normal state, turns ON the R,G,B signals output from the graphic controller **32** by setting the R,G,B output register to an ON state, and turns ON the HDD **81** if there is a signal input to the CPU **2** from the input/output controller **7**, the IDE controller **8** and the expansion function block **9** by the input by the keyboard **71**, input by the mouse **72**, input by the infrared port **74**, access of the FDD **73**, access of the HDD **81**, access of the compact disk ROM **82**, access of the fax/modem card **92** or access of the network card **93** at step **419**.

However, the computer system maintains the graphic off mode in which any letters or image information is not displayed on the screen of the display unit **33** since the R,G,B signals output from the graphic controller **32** are not continually input to the display unit **33** owing to the graphic cut-off signal output from the input/output controller **7**.

The user enters the password in the graphic off mode in which any letters or image information is not displayed on the screen of the display unit **33** of display or monitor **3**. The input/output controller **7** stops outputting the graphic cut-off signal and directs the R,G,B signals from the graphic controller **32** to the display unit **33** for a visual display so that the user may see the screen, and the mode of the computer system is converted into the full power-on mode if the input password is correct after the input/output controller **7** checks the password input by the user in the graphic off mode. However, the input/output controller **7** outputs the graphic cut-off signal continually so that the user can not see the screen if the correct password is not input, and maintains the graphic off mode in which the R,G,B signals from the graphic controller **32** can not be input to the display unit **33**.

The chip set **4** converts the mode of the computer system into the mode in which the power to the CPU **2**, the display **3**, the FDD **73**, the HDD **81** and the other sub-systems are turned OFF at step **423** if there is no signal inputted to the CPU **2** from the input/output controller **7**, the IDE controller **8** and the expansion function block **9** by the input by the keyboard **71**, input by the mouse input by the infrared port **74**, access of the FDD **73**, access of the HDD **81**, access of the compact disk ROM **82**, access of the fax/modem card **92** or access of the network card **93** for a predetermined time set for the suspend mode in the graphic mode at step **421**.

The chip set **4** senses the state of the power switch if the mode of the computer system converts to the suspend mode. A process routine jumps to the step for performing the POST procedure if the power switch is turned ON, and the computer system is booted again. The chip set **4** maintains the power OFF state if the power switch is not turned ON at step **425**.

The present invention relates to an executive routine when suspend information is stored in an auxiliary memory. When the suspend information is stored in a main memory, steps can be added to determine whether there is access to the CPU for the predetermined time after step **425** and to turn OFF the power. In addition, the timer of the present invention and its equivalent measures the standby operation time if the computer system operates in the standby mode for a predetermined time and outputs the graphic off signal.

As described above, the computer system of the present invention has an advantage in that information is kept confidential by adding the graphic off mode between the standby mode and the suspend mode when the computer system operates in the standby mode for the predetermined time. In addition, information can be secured since a password is checked in the graphic off mode in which the letters or the image information may not be displayed.

While there have been illustrated and described what are considered to be preferred embodiments of the present invention, it will be understood by those skilled in the art that various changes and modifications may be made, and equivalents may be substituted for elements thereof without departing from the true scope of the present invention. In addition, many modifications may be made to adapt a particular situation to the teaching of the present invention without departing from the central scope thereof Therefore, it is intended that the present invention not be limited to the particular embodiment disclosed as the best mode contemplated for carrying out the present invention, but that the present invention includes all embodiments falling within the scope of the appended claims.

What is claimed is:

1. A computer system for controlling a display, the computer system having a central processing unit, a memory, a system bus and a display, comprising:

a power controller for converting an operation mode of the computer system into a power management mode, said power management mode representing one of a power-on mode, a standby mode, a graphic off mode, and a suspend mode according to an access state of the computer system, said power controller for converting the computer system into said standby mode when power is applied to the computer system and there is no access to the computer system, for converting the computer system to said graphic off mode in which a screen-display state of said display is controlled according to input of a password, and for converting the computer system into said suspend mode when the computer system is not accessed for a predetermined time during said graphic off mode; and

a screen controller for converting the screen display state of said display according to a designated said power management mode, and said screen controller for controlling the screen display state of said display according to input of a password when the computer system is accessed in said graphic off mode, the computer system checking an input password when entered by a user in said graphic off mode and, when the input password entered in said graphic off mode is a correct password, the computer system by said screen controller then controlling the screen display state to permit a visual display on said display.

2. The computer system of claim 1, further comprising a timer for measuring a standby operation time when the computer system operates in said standby mode for a predetermined time, and said timer generating when said predetermined time in said standby mode has passed a graphic off signal to said screen controller to enter said graphic off mode.

3. The computer system of claim 2, further comprised of said screen controller controlling the screen display state of said display by the graphic off signal input from said timer, and said screen controller controlling the screen display state of said display by a graphic cut-off signal according to the input password.

4. A method for controlling a screen display state of a computer system, comprising the steps of:

converting the computer system into a standby mode when power is applied to the computer system and there is no access to the computer system;

converting the screen display state of a display when there is no access to the computer system for a predetermined time during said standby mode, and converting the computer system to a graphic off mode in which the screen display state of said display is controlled according to input of a password when the computer system in said graphic off mode is again accessed;

checking by the computer system an input password when entered by a user in said graphic off mode and controlling the screen display state by the computer system to permit a visual display on said display when the input password entered in said graphic off mode is a correct password; and

converting the computer system into a suspend mode when the computer system is not accessed for a predetermined time during said graphic off mode.

5. The method of claim 4, further comprised of the screen display state of the display being controlled by a graphic cut-off signal output from an input/output controller to a graphic controller.

6. A method for controlling power supply to a computer system having a computer, a monitor and input devices, said method comprising the steps of:

initializing said computer system upon activation of power;

requesting entry of a password when the password is set at the time of a computer setup;

when the password is entered correctly, supplying power to the computer system for use in a power-on mode of operation;

determining whether there is activity from input devices indicating that the computer system is in use for a first time period;

when there is activity from the input devices indicating that the computer system is in use during the first time period, maintaining the power supply to the computer system;

when there is no activity from the input devices indicating that the computer system is not in use during the first time period, converting the computer system into a standby mode of operation;

determining whether there is further activity from the input devices for a second time period;

when there is activity from the input devices during the second time period, resupplying power back to the computer system and maintaining the power supply to the computer system for use;

when there is no further activity from the input devices during the second time period, converting the computer system into a graphic-off mode of operation shutting off a visual display on the monitor;

determining whether there is yet activity from the input devices for a third time period;

when there is activity from the input devices during the third time period, requesting entry of said password before resupplying power back to the computer system for use in the power-on mode;

when there is no activity from the input devices during the third time period, converting the computer system in a suspend mode of operation.

7. The method of claim 6, further comprised of supplying power to the computer system for use in said power-on mode of operation without requesting entry of said password when the password is not set at the time of the computer setup.

8. A computer system, comprising:

a main computer containing a controller and auxiliary devices;

a monitor physically separated from but electrically connected to said main computer;

input devices connected to said main computer; and

said controller controlling power supply and a screen display state of said monitor by the steps of:

initializing said computer system upon activation of power;

requesting entry of a password when the password is set at the time of a computer setup;

when the password is entered correctly, supplying power to the computer system for use in a power-on mode of operation;

determining whether there is activity from input devices indicating that the computer system is in use during a first time period;

when there is no activity from the input devices indicating that the computer system is not in use during the first time period, converting the computer system into a standby mode of operation;

determining whether there is further activity from the input devices for a second time period;

when there is no further activity from the input devices during the second time period, converting the computer system into a graphic-off mode of operation shutting off a visual display on the monitor;

determining whether there is yet activity from the input devices for a third time period;

when there is activity from the input devices during the third time period, requesting entry of said password before resupplying power back to the computer system for use in the power-on mode;

when there is no activity from the input devices during the third time period, converting the computer system in a suspend mode of operation.

9. The computer system of claim **8**, further comprised of said controller supplying power to the computer system for use in said power-on mode of operation without requesting entry of said password when the password is not set at the time of the computer setup.

10. The computer system of claim **8**, further comprised of said controller maintaining the power supply to the computer system, when there is activity from the input devices indicating that the computer system is in use during the first time period.

11. The computer system of claim **8**, further comprised of said controller resupplying power back to the computer system and maintaining the power supply to the computer system for use, when there is activity from the input devices during the second time period.

12. The computer system of claim **10**, further comprised of said controller resupplying power back to the computer system and maintaining the power supply to the computer system for use, when there is activity from the input devices during the second time period.

13. The computer system of claim **9**, further comprised of said controller maintaining the power supply to the computer system, when there is activity from the input devices indicating that the computer system is in use during one of the first time period and the second time period.

* * * * *

US006111517A

United States Patent [19]

Atick et al.

[11] **Patent Number: 6,111,517** ✓

[45] **Date of Patent: Aug. 29, 2000**

[54] **CONTINUOUS VIDEO MONITORING USING FACE RECOGNITION FOR ACCESS CONTROL**

[75] Inventors: **Joseph J. Atick**; **Paul A. Griffin**, both of New York, N.Y.; **A. Norman Redlich**, Metuchen, N.J.

[73] Assignee: **Visionics Corporation**, Jersey City, N.J.

[21] Appl. No.: **08/774,556**

[22] Filed: **Dec. 30, 1996**

[51] **Int. Cl.**^{7} **G07D 7/00**

[52] **U.S. Cl.** **340/825.34**; 382/118

[58] **Field of Search** 340/825.34, 825.31; 382/115, 118, 203, 276; 348/156, 14; 902/3; 704/273, 1

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,449,189	5/1984	Feix et al.	382/118 X
4,712,103	12/1987	Gotanda	340/835.31
4,858,000	8/1989	Lu .	
4,975,969	12/1990	Tal	340/825.34 X
4,993,068	2/1991	Piosenka et al.	340/825.34 X
5,031,228	7/1991	Lu .	
5,164,992	11/1992	Turk et al. .	
5,189,691	2/1993	Dunlap	348/14 X
5,229,764	7/1993	Matchett et al.	340/825.34
5,331,544	7/1994	Lu et al. .	
5,386,103	1/1995	DeBan et al.	235/379
5,432,864	7/1995	Lu et al.	382/118
5,561,718	10/1996	Trew et al.	382/118
5,771,307	6/1998	Lu et al. .	
5,835,616	11/1998	Lobo et al. .	
5,991,429	11/1999	Coffin et al. .	
6,009,210	12/1999	Kang .	

FOREIGN PATENT DOCUMENTS

WO 93/11511	6/1993	WIPO .

OTHER PUBLICATIONS

"FERET (Face Recognition Technology) Recognition Algorithm Development and Test Results;" P. Jonathon Phillips, Patrick J, Rauss, abd Sandor Z. Der; Army Research Laboratory, Report No. ARL–TR–995, 72 pages, Oct. 1996.

Primary Examiner—Edwin C. Holloway, III
Attorney, Agent, or Firm—Pennie & Edmonds LLP

[57] **ABSTRACT**

A continuous monitoring system for regulating access to a computer system or other restricted environment is disclosed. The system employs real-time face recognition to initially detect the presence of an authorized individual and to grant the individual access to the computer system. In some embodiments, the system also employs real-time face recognition to continuously or periodically track the continued presence of the authorized individual. Access to the computer system is revoked when the individual's presence is no longer detected. In other embodiments, the system employs a screen saver program to deny access to the computer system when a predetermined period of user inactivity is detected. Other aspects of the invention include a stranger detector which warns the authorized individual of the approach of an unauthorized individual, a multimedia messaging center which permits unauthorized individuals to leave messages for authorized individuals, and an adaptive enrollment program which permits the system to update the stored video images of authorized individuals to reflect the individuals' current appearance.

48 Claims, 11 Drawing Sheets

Microfiche Appendix Included
(22 Microfiche, 2070 Pages)

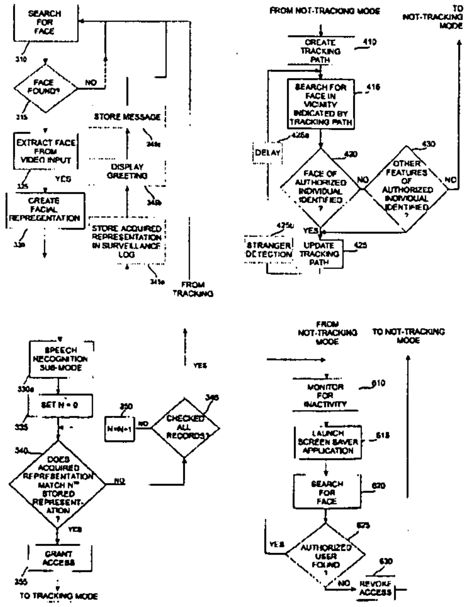


Fig. 1

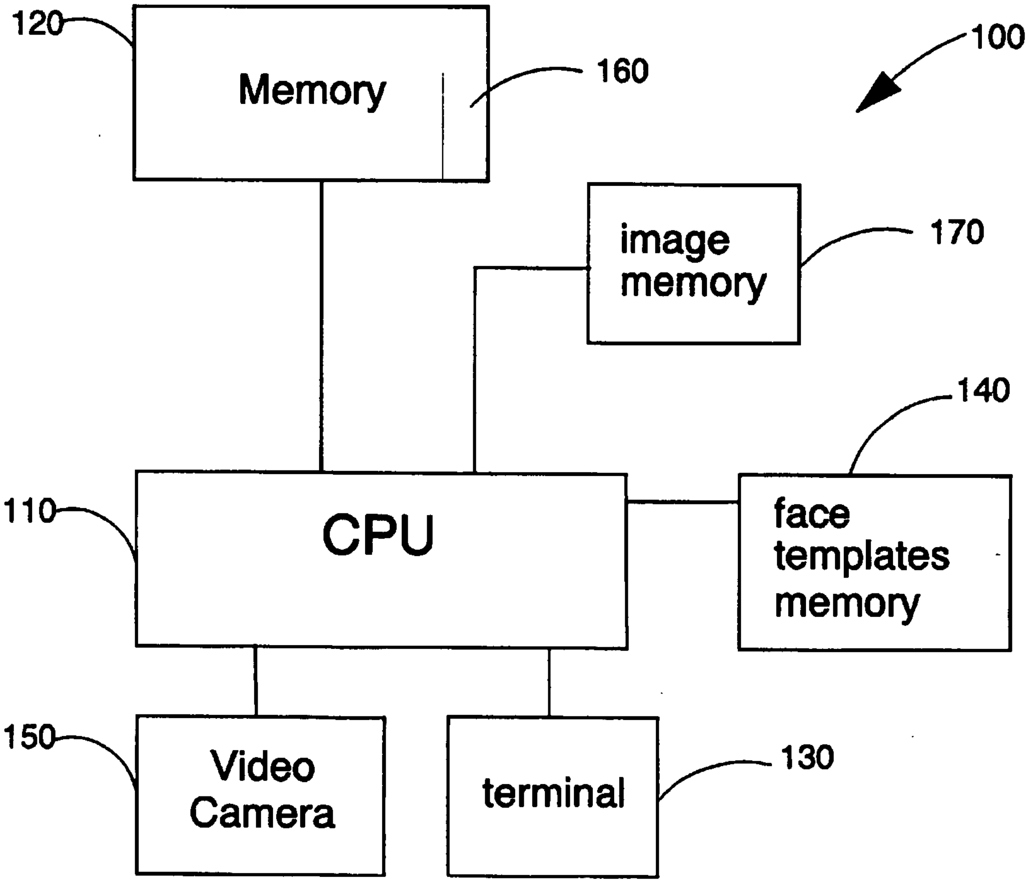

120
Memory
160
100
image memory
170
140
110
CPU
face templates memory
150
Video Camera
terminal
130

Fig. 2

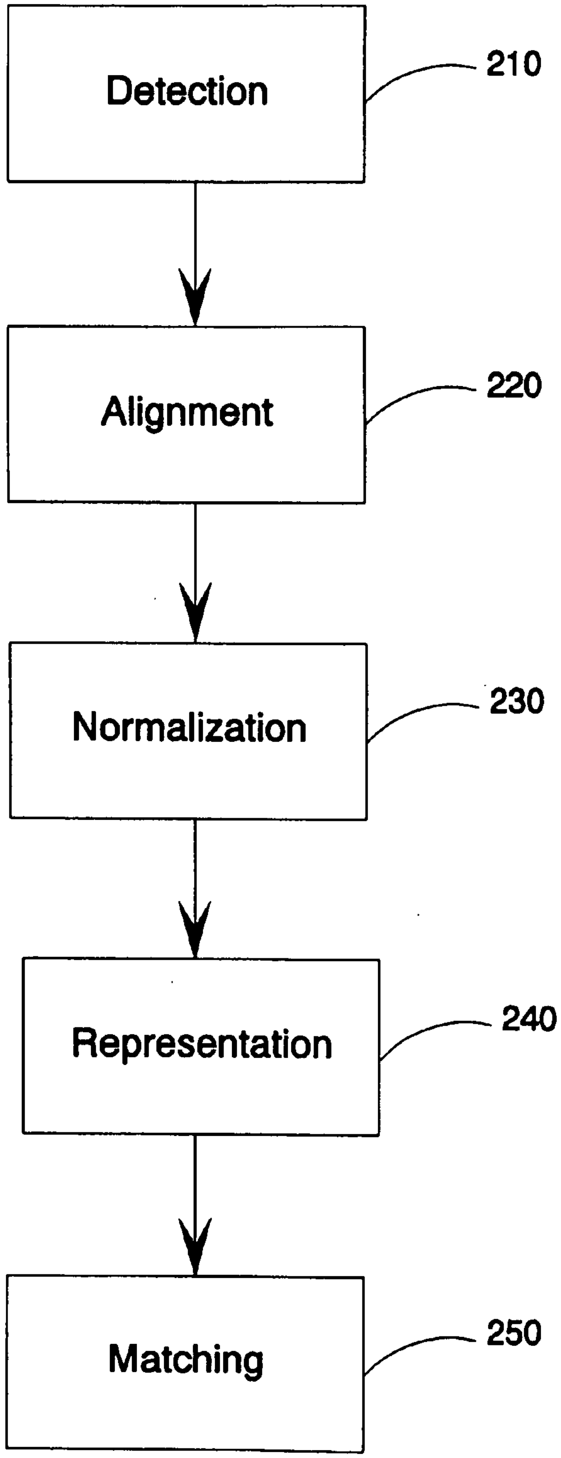

Detection
210
Alignment
220
Normalization
230
Representation
240
Matching
250

FIG. 3A

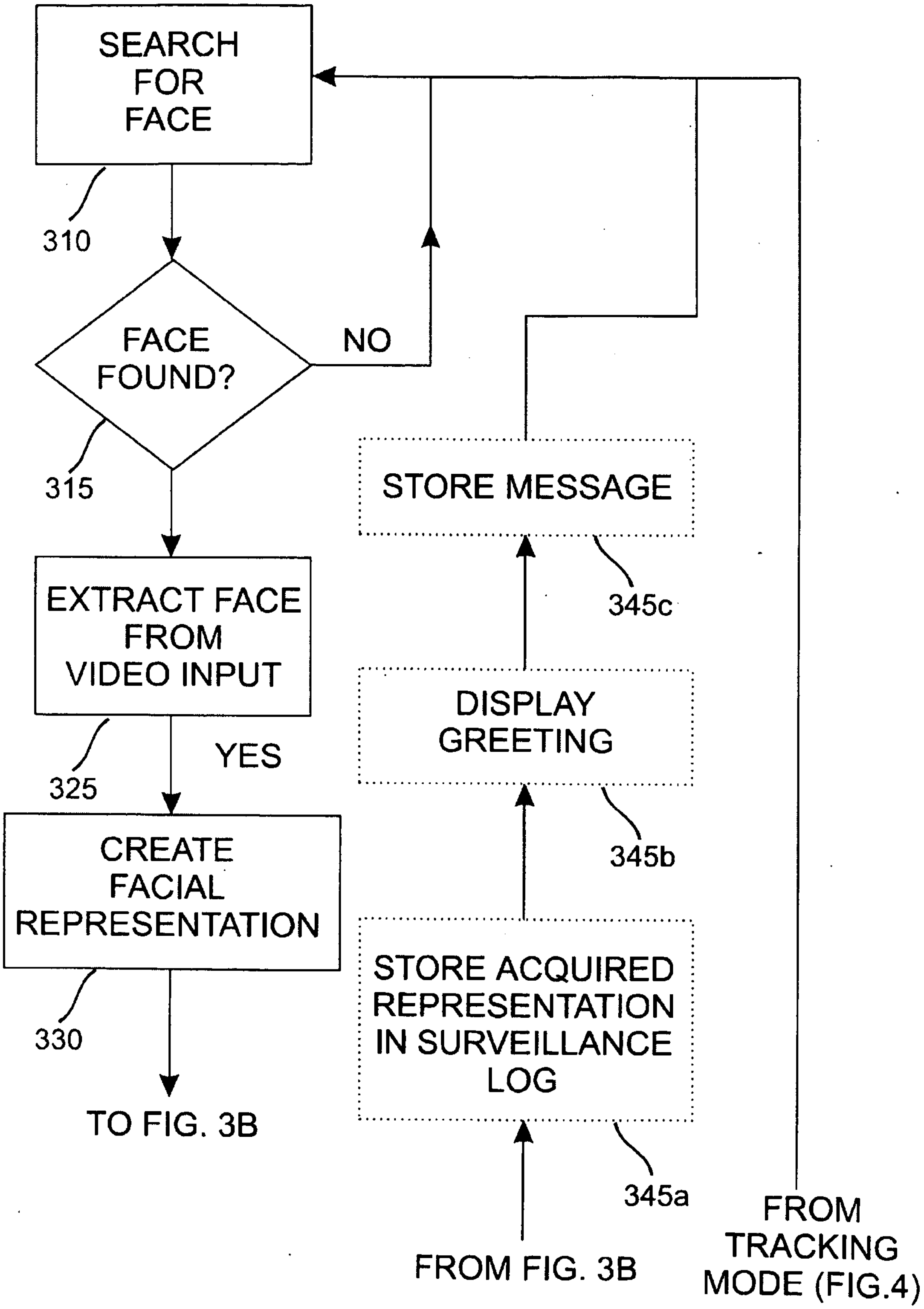

SEARCH FOR FACE
310
FACE FOUND?
315
NO
EXTRACT FACE FROM VIDEO INPUT
325
YES
CREATE FACIAL REPRESENTATION
330
TO FIG. 3B
STORE MESSAGE
345c
DISPLAY GREETING
345b
STORE ACQUIRED REPRESENTATION IN SURVEILLANCE LOG
345a
FROM FIG. 3B
FROM TRACKING MODE (FIG.4)

FIG. 3B

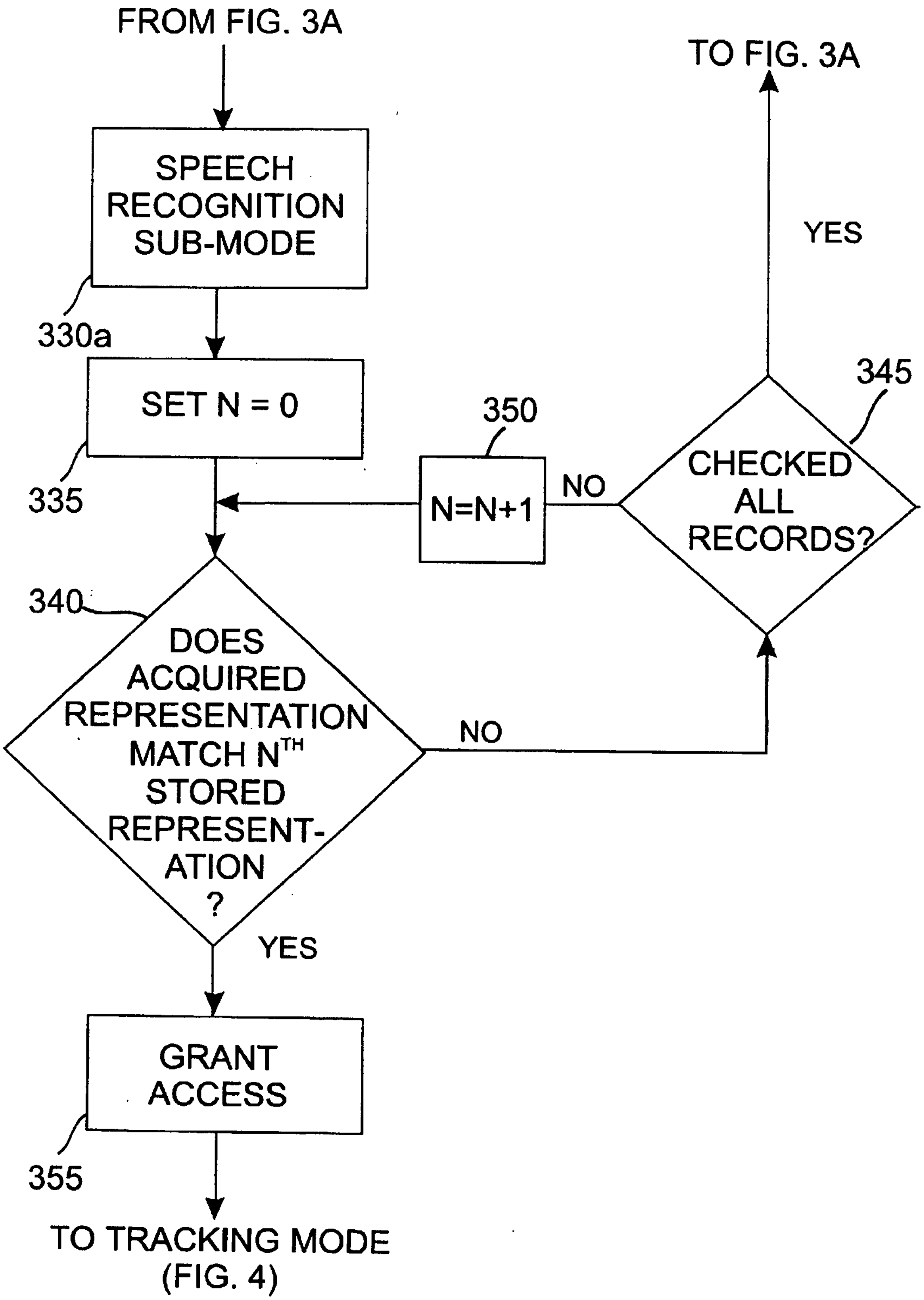

FROM FIG. 3A
TO FIG. 3A
SPEECH RECOGNITION SUB-MODE
330a
SET N = 0
335
YES
345
350
N=N+1
NO
CHECKED ALL RECORDS?
340
DOES ACQUIRED REPRESENTATION MATCH NTH STORED REPRESENT- ATION ?
NO
YES
GRANT ACCESS
355
TO TRACKING MODE (FIG. 4)

FIG. 4

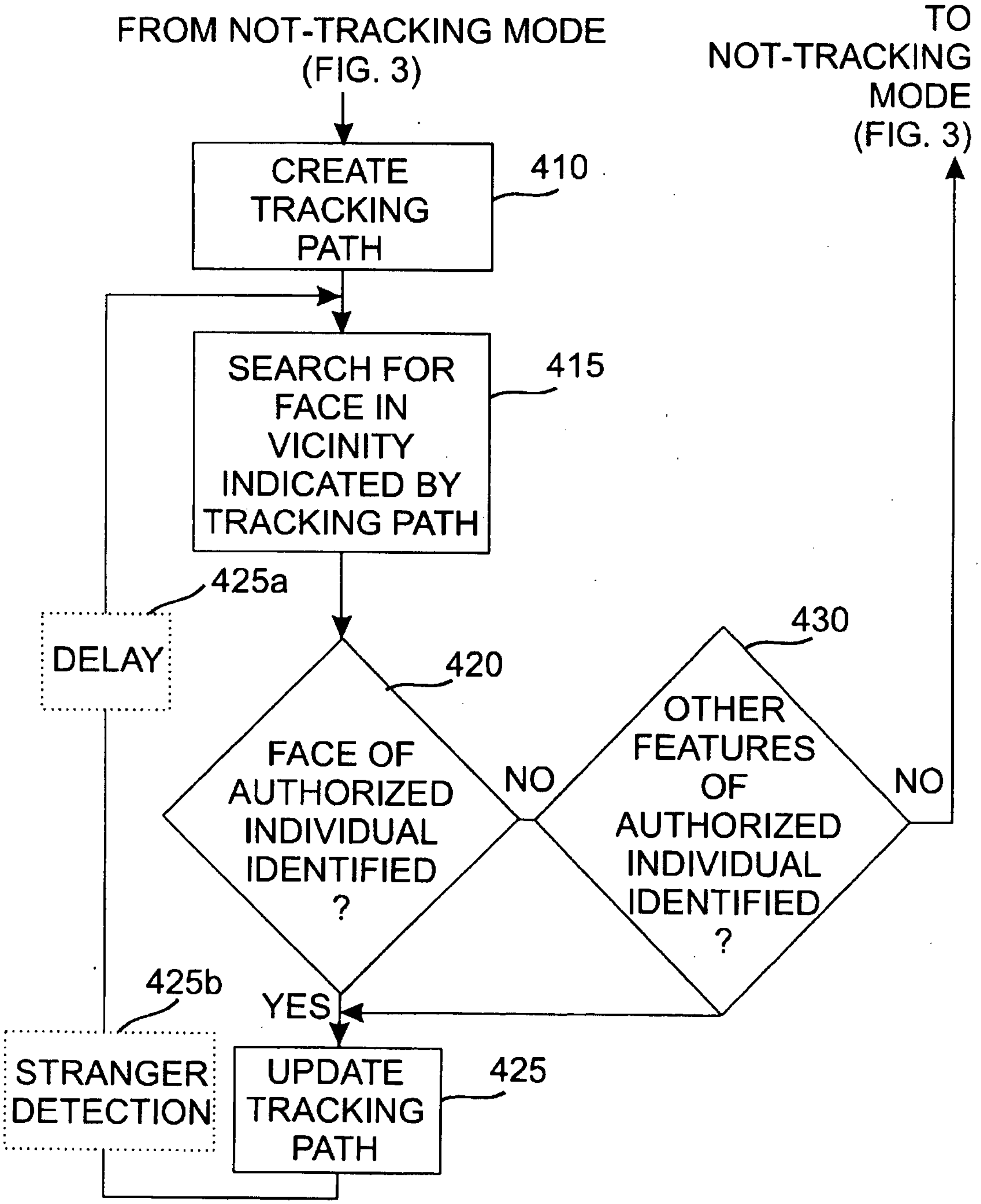

FROM NOT-TRACKING MODE (FIG. 3)
CREATE TRACKING PATH
410
SEARCH FOR FACE IN VICINITY INDICATED BY TRACKING PATH
415
425a
DELAY
420
FACE OF AUTHORIZED INDIVIDUAL IDENTIFIED ?
NO
430
OTHER FEATURES OF AUTHORIZED INDIVIDUAL IDENTIFIED ?
NO
TO NOT-TRACKING MODE (FIG. 3)
YES
425b
STRANGER DETECTION
UPDATE TRACKING PATH
425

FIG 5

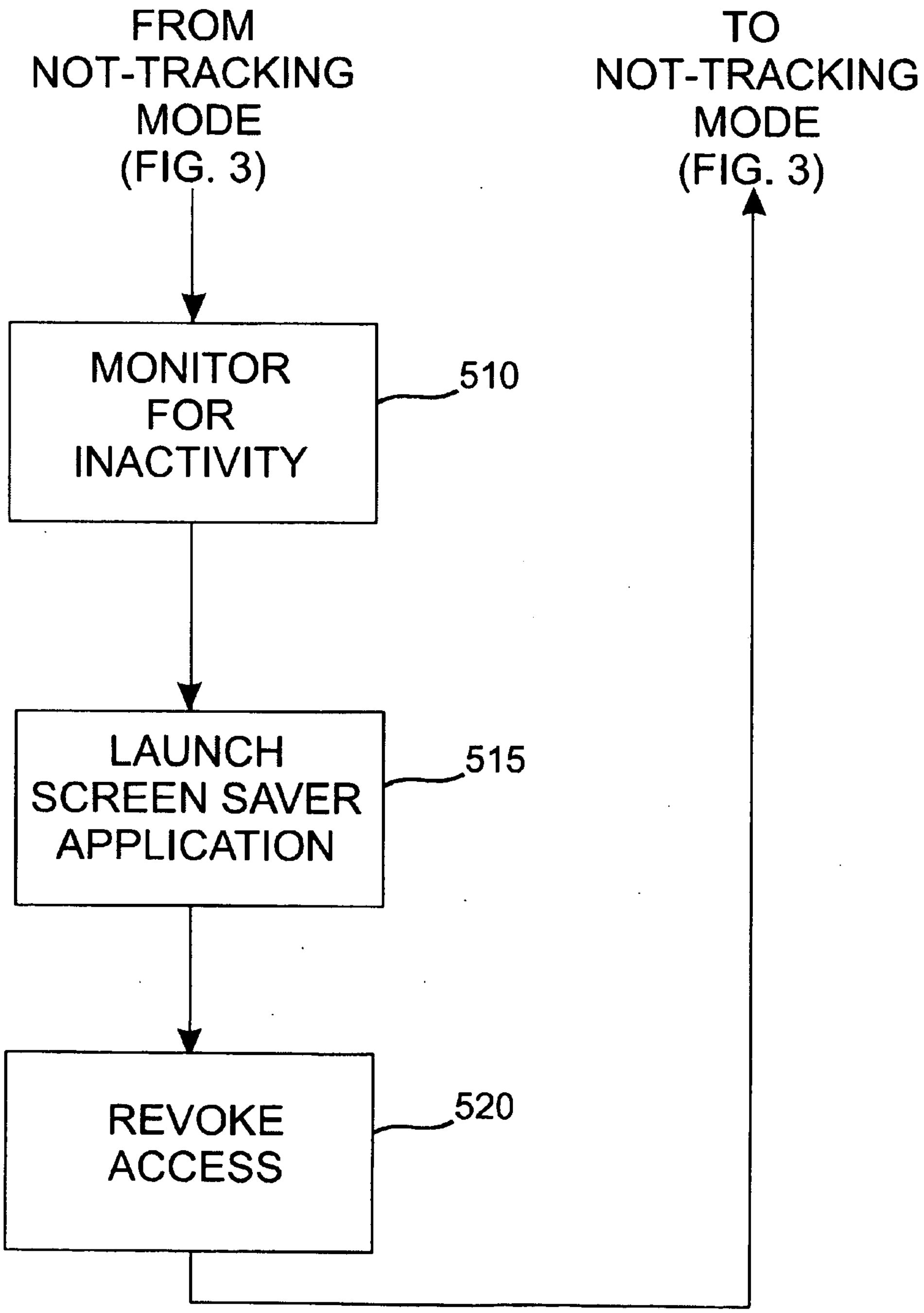

FROM NOT-TRACKING MODE (FIG. 3)
TO NOT-TRACKING MODE (FIG. 3)
MONITOR FOR INACTIVITY
510
LAUNCH SCREEN SAVER APPLICATION
515
REVOKE ACCESS
520

FIG. 6

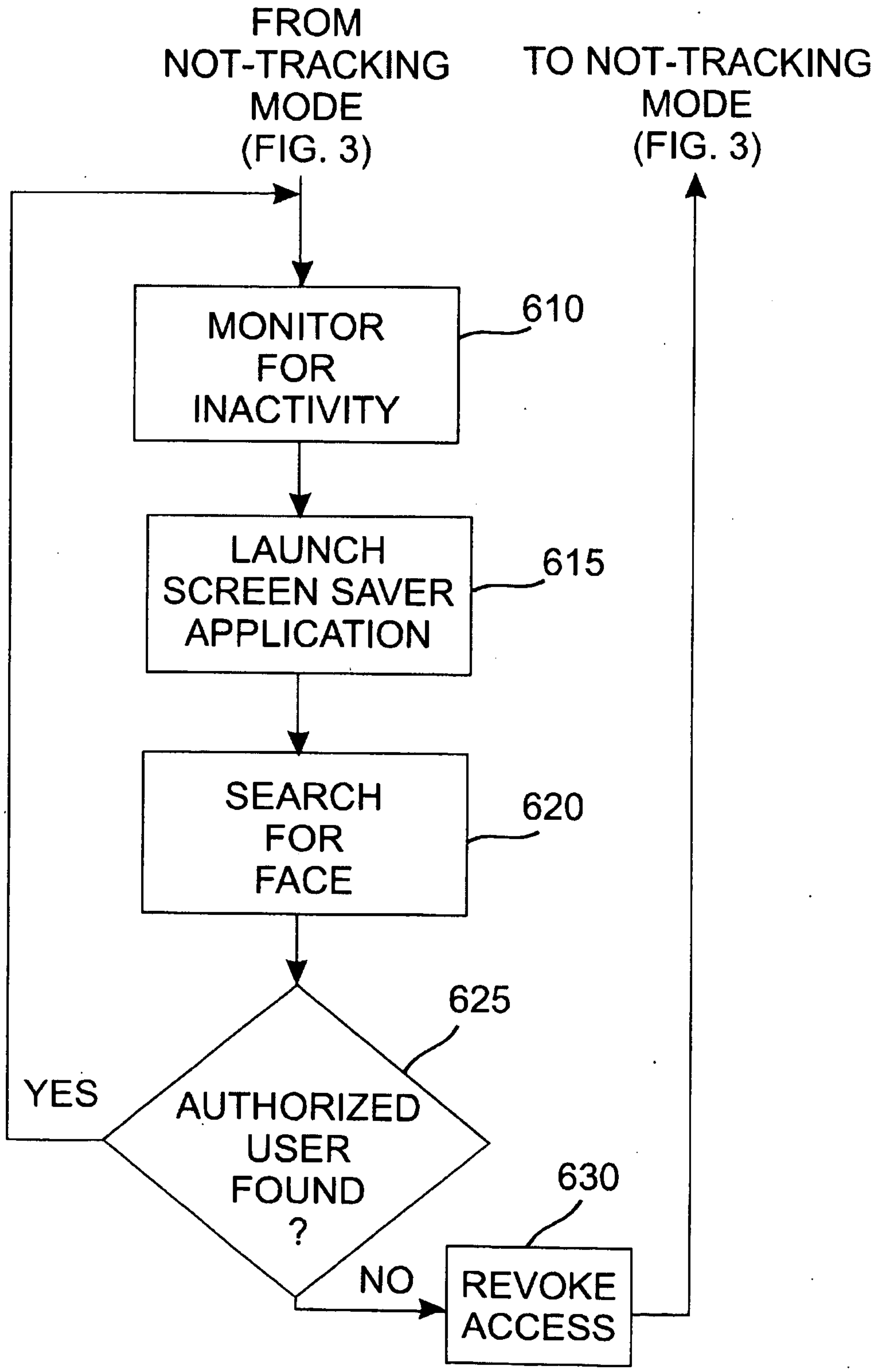

FROM NOT-TRACKING MODE (FIG. 3)
TO NOT-TRACKING MODE (FIG. 3)
MONITOR FOR INACTIVITY
610
LAUNCH SCREEN SAVER APPLICATION
615
SEARCH FOR FACE
620
AUTHORIZED USER FOUND ?
625
YES
NO
REVOKE ACCESS
630

Fig. 7

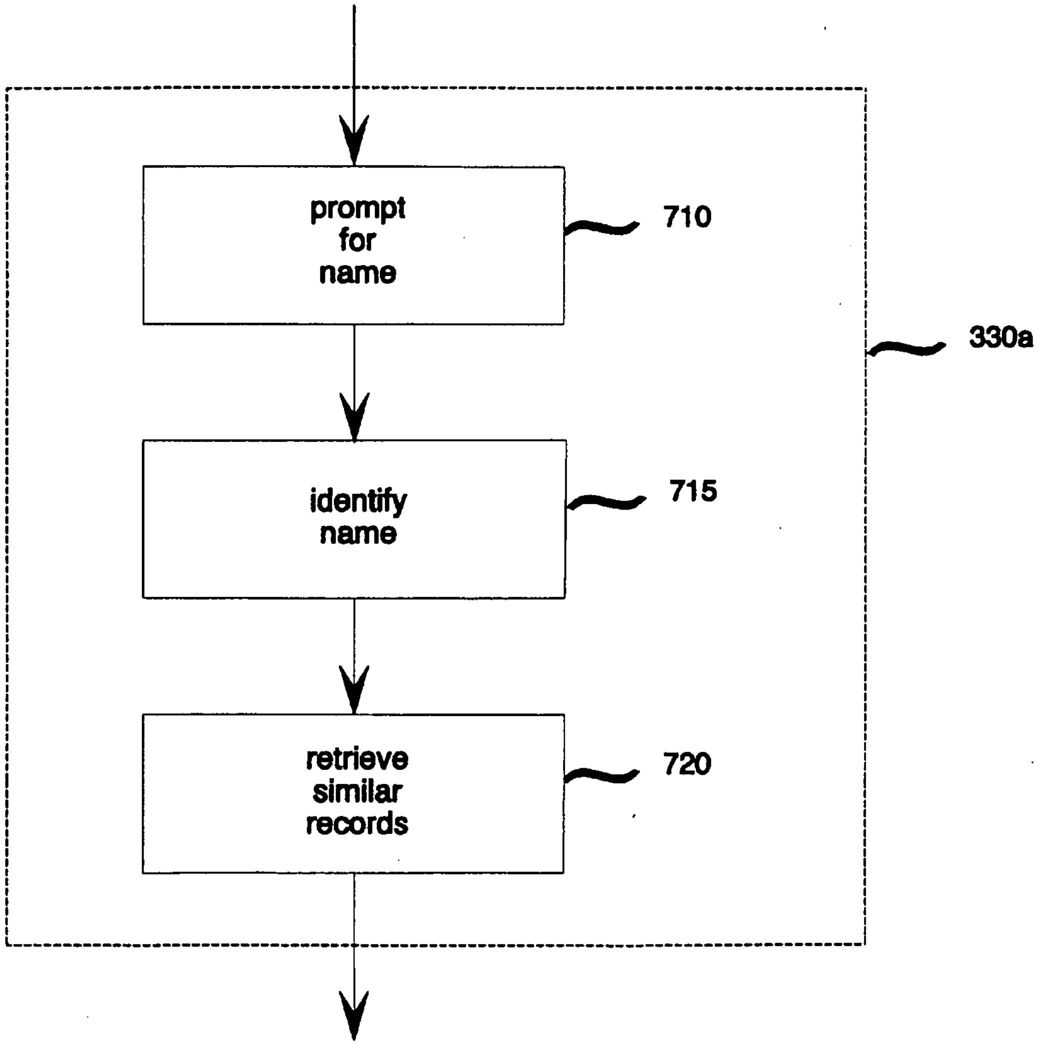

prompt for name
710
identify name
715
retrieve similar records
720
330a

Fig. 8

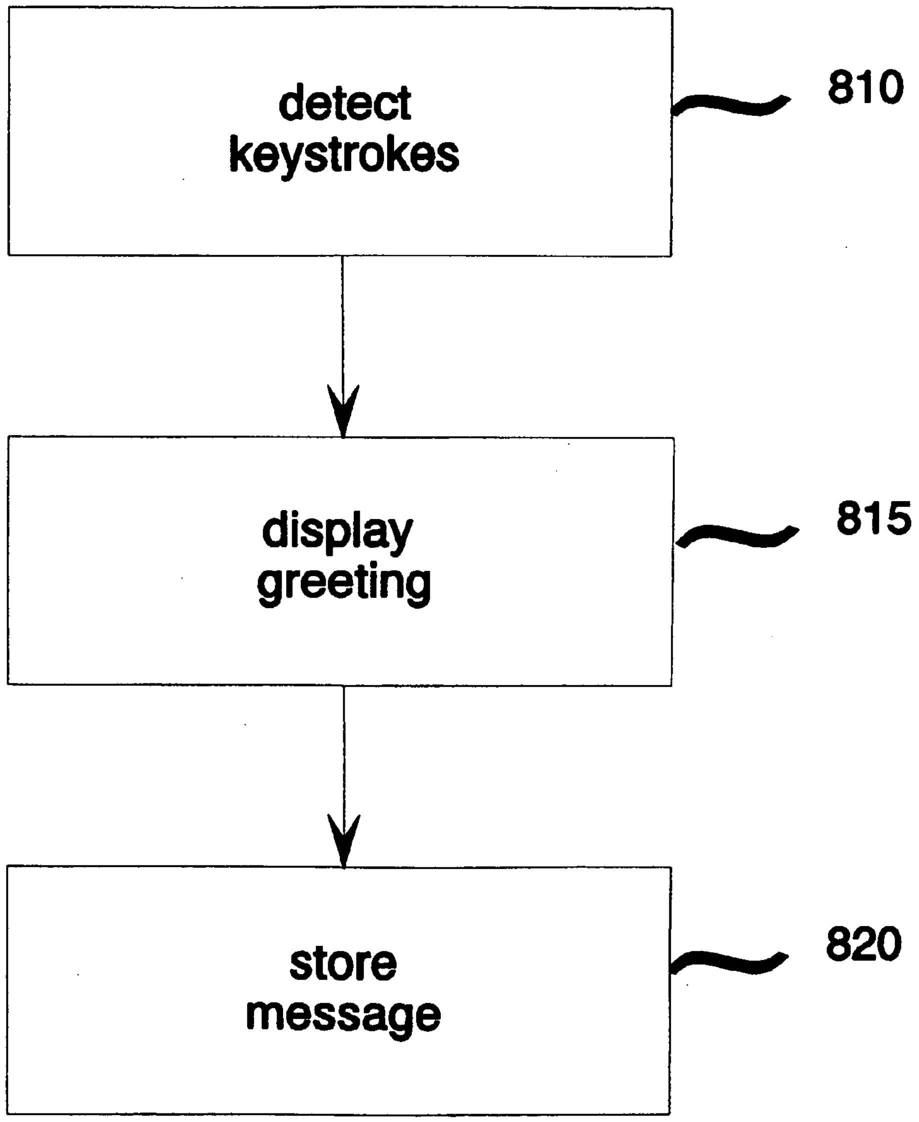

detect keystrokes
810
display greeting
815
store message
820

Fig. 9

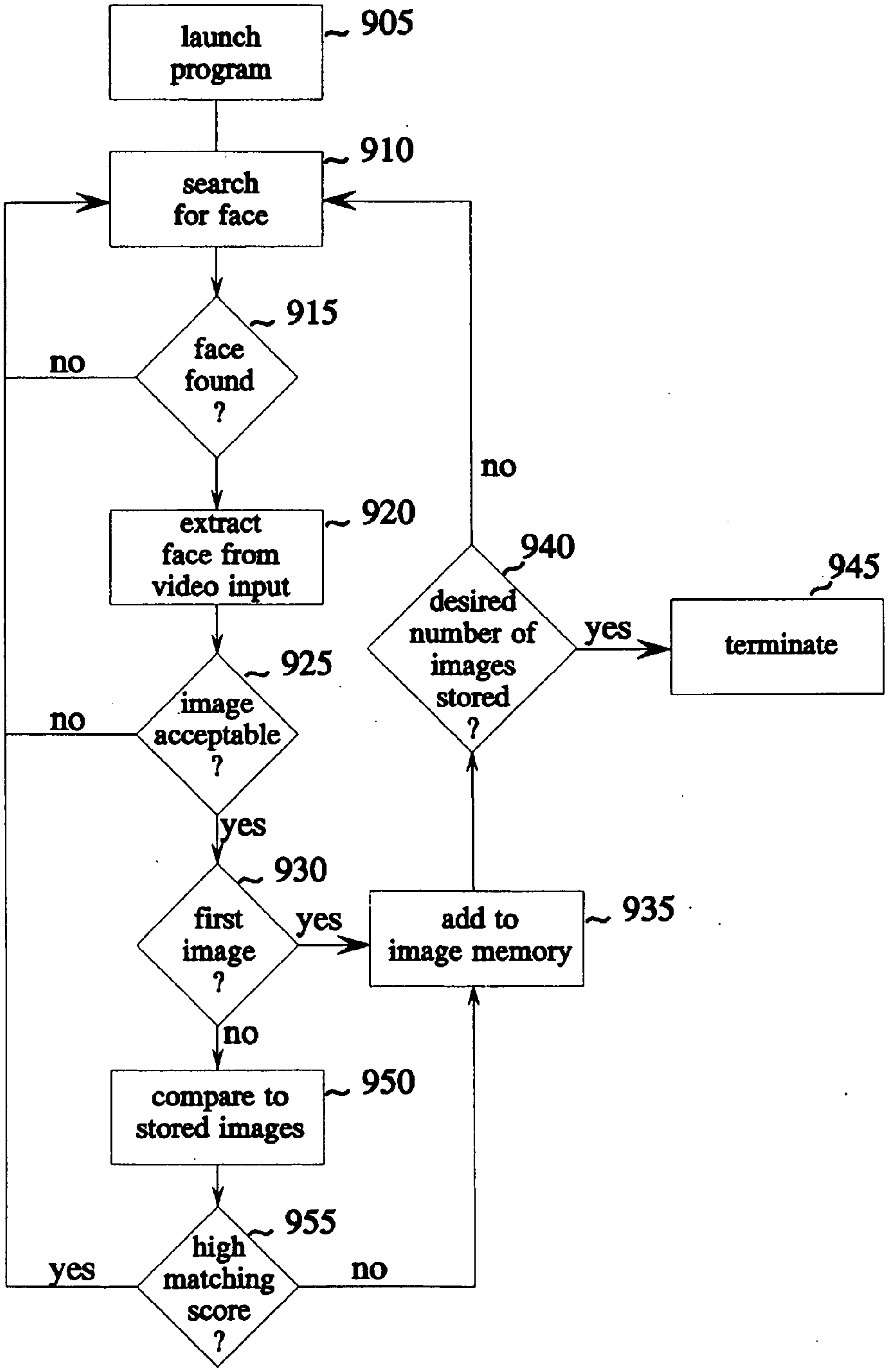
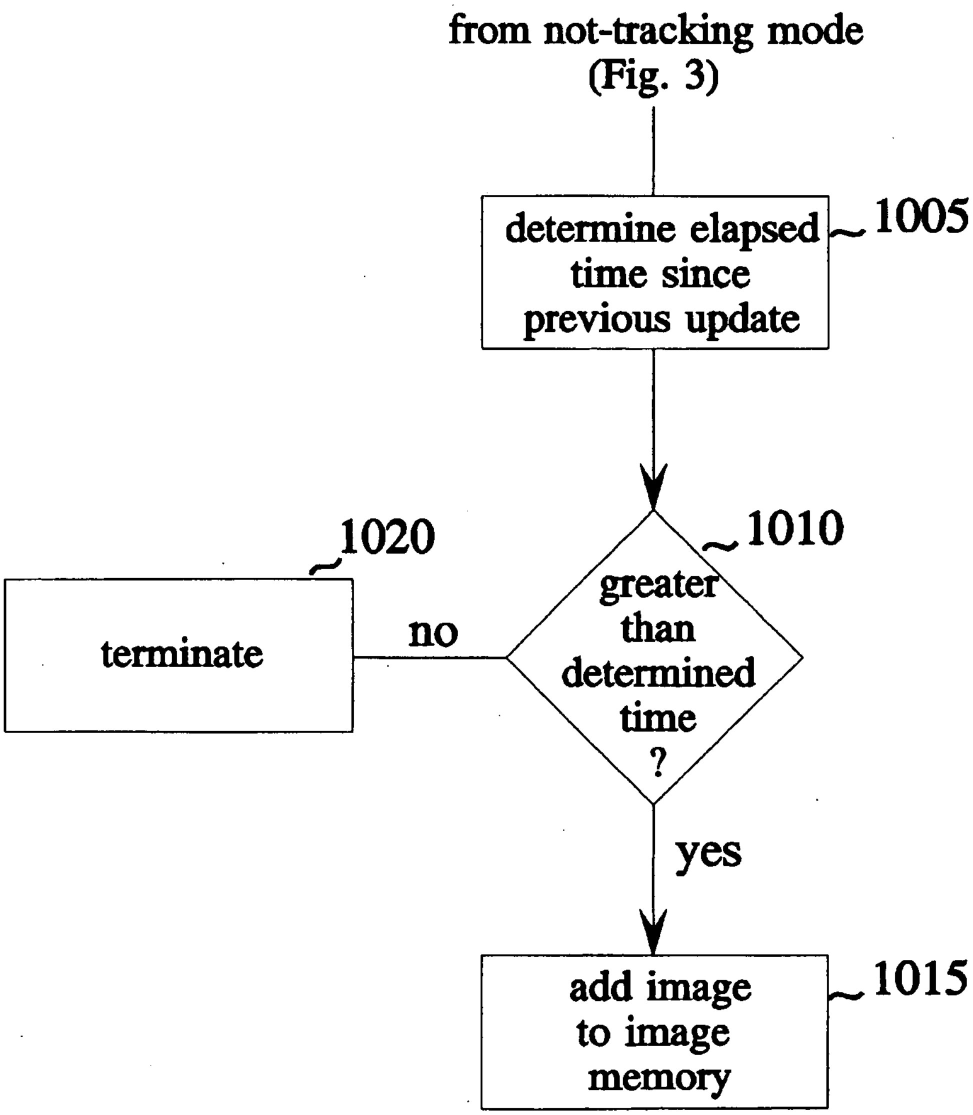

launch program
905
search for face
910
face found ?
915
no
extract face from video input
920
image acceptable ?
925
no
yes
first image ?
930
yes
no
add to image memory
935
desired number of images stored ?
940
no
yes
terminate
945
compare to stored images
950
high matching score ?
955
yes
no

Fig. 10


from not-tracking mode
(Fig. 3)
determine elapsed time since previous update
1005
greater than determined time ?
1010
no
terminate
1020
yes
add image to image memory
1015

CONTINUOUS VIDEO MONITORING USING FACE RECOGNITION FOR ACCESS CONTROL

COPYRIGHT AUTHORIZATION

FIELD OF THE INVENTION

The invention relates to a system employing real-time face recognition software to regulate and monitor access to computers and other restricted environments.

BACKGROUND OF THE INVENTION

Many computer systems permit access only to authorized users. This is generally accomplished by requiring those seeking to use the system to prove that they are authorized to do so. Proof of authorization can take many forms. Often, the user must provide a name or initials and a password or Personal Identification Number (PIN) before being permitted to use the system. Other systems require the user to insert a magnetic card or similar "key" into a reader which verifies that the cardholder is authorized to use the system. Still others evaluate some biometric characteristic of the user, such as the user's voice print.

All such access control systems, however, suffer from several drawbacks. The most important is that they merely restrict initial access to the computer system. Once a user has gained access, continued use of the system is possible by someone else when the authorized user leaves the computer system unattended. This decreases the security of the system for several reasons. If the user leaves the computer unattended, an unauthorized user may gain access to sensitive data stored in the computer system. Moreover, the unauthorized user might also be in a position to modify or even erase data stored in the computer system.

To avoid this possibility, wary authorized users may choose to exit the system even when stepping away from the computer for only a short time. This, too, has a drawback: the authorized user must reenter the computer system when he returns, a process which may take several minutes. Furthermore, this tactic does not permit continued running of application programs such as spreadsheets while the user is away. As a result, users may end up "standing guard" at their computers when running sensitive spreadsheets and other programs.

Second, presently available access control systems do not offer convenient hands-off or passive operation, since they require the active participation of the user before entry is granted. Therefore, in addition to the inconvenience of remembering a password or of carrying a magnetic card, users suffer the additional inconvenience of typing the password into a keyboard or swiping the magnetic card, before access is granted.

Furthermore, security systems that use passwords or cards can be compromised since a password can be discovered by an intruder and cards can be stolen.

A need therefore exists in the art for a security system without the above drawbacks. In particular, there is a need for a convenient passive security system which continuously monitors the identity of an authorized user and prevents access to a computer system without shutting the computer system down when it is determined that the authorized user has left the computer unattended.

In addition, the need for a continuous monitoring system exists not only with respect to virtual environments such as a computer system, but more generally extends to other restricted environments, including physical environments such as bank vaults.

OBJECTS AND SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a security system which continuously monitors the identity of an authorized individual and prevents access to a computer system or other restricted environment when it is determined that the authorized individual has left the vicinity of the environment.

It is a further object of the present invention to continuously verify the identity of an authorized user in real time.

It is a further object of the present invention to perform the continuous monitoring in a manner which is passive, i.e., in a manner which does not require the participation of the user.

It is a further object of the present invention to assign an authorization level to each authorized individual and to permit each authorized individual access only to those application programs and data appropriate for the user's authorization level.

It is a further object of the present invention to provide a security system which continuously monitors whether a second person other than the authorized user has approached within reading distance of a display of the computer system and which, upon detection of this circumstance, disables the display or alerts the authorized user of the second person's presence.

It is a further object of the present invention to provide a continuous monitoring system which employs face recognition to passively regulate both initial and continuing access to a computer system.

It is a further object of the present invention to fuse face recognition and speech recognition to provide swift initial access to a computer system.

It is a further object of the present invention to employ the screen saver utility resident in most operating systems to revoke access to a computer system when a significant period of user inactivity is detected.

It is a further object of the present invention to employ the screen saver utility resident in most operating systems to launch a face recognition program which revokes access to a computer system when it fails to identify the continued presence of an authorized individual.

It is a further object of the present invention to employ the screen saver utility resident in most operating systems to launch a motion detection program which revokes access to the computer system when it fails to detect motion in the vicinity of the computer system.

It is a further object of the present invention to provide a video monitoring system which detects the presence of an unauthorized person, and upon detection of this circumstance, displays a greeting to that person and permits the person to leave a message for an authorized person.

These and other objects of the invention are accomplished by a system comprising a video input device coupled to a general purpose computer or other specialized hardware furnished with a face-recognition software program. The face recognition algorithm is capable of identifying faces in real time. The system repeatedly compares the face registered by the video input device with the facial representations of authorized individuals. When the comparison fails to indicate a match, continued access to the computer system is denied.

BRIEF DESCRIPTION OF THE DRAWINGS

The above objects and summary of the invention will be better understood when taken in conjunction with the following detailed description and accompanying drawings in which:

FIG. **1** is a block diagram of a preferred computer system architecture implementing the continuous monitoring system of the present invention;

FIG. **2** is a high level flowchart depicting the steps in face recognition;

FIG. **3** is a flowchart depicting the not-tracking mode of the continuous monitoring system of the present invention;

FIG. **4** is a flowchart depicting the tracking mode of the continuous monitoring system of the present invention;

FIG. **5** is a flowchart depicting an inactivity detection mode;

FIG. **6** is a flowchart depicting an alternative inactivity detection mode;

FIG. **7** is a flowchart depicting a speech recognition sub-mode of the not-tracking mode shown in FIG. **3**;

FIG. **8** is a flowchart depicting the operation of a multimedia messaging center which does not employ face recognition;

FIG. **9** is a flowchart depicting an enrollment program for storing the facial images of individuals authorized to have access to a restricted environment; and

FIG. **10** is a flowchart depicting an adaptive enrollment program for updating the stored images of individuals authorized to have access to a restricted environment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to the drawings, FIG. **1** shows a computer system **100** which comprises a CPU **110**, a memory **120**, and input/output (I/O) means such as terminal **130**. Memory **120** stores application programs run on CPU **110** as well as other data and information.

Computer system **100** also comprises an image memory **170**, a face templates memory **140** and a video input device such as video camera **150**. As described more fully below, image memory **170** stores one or more facial images of each individual authorized to have access to computer system **100**. When computer system **100** is initialized, the stored images of each authorized individual are converted to a facial representation or template. These templates are stored in face templates memory **140**. If desired, image memory **170** and face templates memory **140** may be implemented as part of memory **120**. Memory **120** also stores a real-time face recognition software program **160**.

In a preferred embodiment, the video camera **150** is positioned such that a user sitting in front of terminal **130** would be in the field of view of video camera **150**. As explained in more detail below, program **160** enables computer system **100** to match facial images transmitted by video camera **150** against facial representations stored in face templates memory **140** and to ascertain whether persons in the field of view of video camera **150** are authorized to have access to computer system **100**.

Before describing the function of the continuous monitoring system of the present invention, a short review of the principal steps in face recognition would be useful. As shown in FIG. **2**, face recognition can be broken down into a sequence of discrete tasks. In detection step **210**, the face recognition system searches the field of view of a video input device for faces.

In a real-time system—such as the system of the present invention—face detection must be accomplished in a fraction of a second. This is a challenge since the search area consists of the entire field of view of video camera **150** which is often as large as 640 by 480 pixels. Current algorithms meet this challenge and accomplish real-time detection by employing either a multiscale search strategy, a multicue search strategy, or both, which permits the entire field of view to be searched at a considerably higher speed than would otherwise be possible.

Multiscale search algorithms initially search for faces in low resolution and switch to high resolution only when the low resolution search indicates a head-like shape. Multicue search algorithms on the other hand, initially search for easily detected cues which indicate the presence of a face. For example, the presence of a face in the field of view often generates discontinuities in the spatial, temporal, and color domains of the video image. Multicue algorithms search for such discontinuities and further examine only those areas where the discontinuities are significant. Software programs for performing real-time face detection using a multiscale and multicue search strategy are commercially available. One such program is.the C++ function CHead::FindHeadPosition of the FaceIt Developer Kit. A copy of the object code and a description of the Application Programming Interface (API) for this function is found in microfiche appendix A hereto. A person skilled in the art can use CHead to perform face detection from video input as specified by the API.

Once a face has been detected, the face recognition system performs alignment step **220** to precisely determine the head's position, size, and pose. This step requires detailed shape and feature detection. Software programs for performing alignment step **220** are also commercially available. One such program is the function CAlignment::FindAlignedPosition of the FaceIt Developer Kit. A copy of the object code of this program is also found in microfiche appendix A hereto.

Next, the face recognition system performs normalization step **230**. Here, the head is normalized by scaling, rotating, and warping, so that the face can be registered and mapped into a canonical size and pose regardless of its location and distance from video camera **150**. Normalization is also performed with respect to lighting variability. Normalization step **230**, too, can be performed using commercially available software programs such as CFace::GetCanonicalImage function of the FaceIt Developer Kit. A copy of the object code of this program is also found in microfiche appendix A hereto.

The fourth step is representation step **240**. Every face recognition system utilizes an internal representation scheme which it employs to translate facial data into a unique coded characterization of the face of each individual. The representation scheme permits relatively simple comparison of acquired facial data with stored facial data to confirm the identity of a particular individual. A preferred embodiment for converting the images stored in image memory 170 into templates suitable for performing face recognition is the function CFace::LoadFace of the FaceIt Developer Kit. A copy of the object code of this function may be found in microfiche Appendix A of this application. In this preferred embodiment, when computer system 100 boots up, it retrieves the images of all authorized users from image memory 170 and converts them to face templates. The system then stores these templates in face templates memory 140 where they remain until computer system 100 is shut down.

The fifth step is matching step 250. In this step the acquired facial representation is compared to at least one stored facial representation and a score is computed which represents the degree to which the acquired representation matches the stored representation. If the score is above a predetermined threshold, a match is declared, and the face in the field of view is identified as belonging to the person associated with the stored facial_representation. Software programs that generate a representation for faces, step 240, and for performing matching step 250 on that representation are commercially available. One such program is the function CFace::IdentifyPerson of the FaceIt Developer Kit. A copy of the object code of this program is also found in microfiche appendix A hereto.

Of course, before a face recognition system can be used, authorized users must be enrolled into the database. A preferred embodiment of an enrollment program that is used by the present invention to store the facial images of authorized individuals into image memory 170 is described below in connection with FIGS. 9 and 10.

The continuous monitoring system of the present invention preferably comprises two modes: a not-tracking mode and a tracking mode. These two modes are described in connection with FIGS. 3 and 4. The continuous monitoring system depicted in FIGS. 3 and 4 is implemented in face recognition software 160 which runs on CPU 110 of computer system 100.

During periods when no one is detected in the field of view of video camera 150, the system remains in not-tracking mode. In this mode, the screen and keyboard of terminal 130 are disabled, thus preventing access to the data or application programs of computer system 100.

The not-tracking mode may be divided into three sub-modes. In the first sub-mode, which comprises steps 310–315 of FIG. 3, the system repeatedly searches for a human face in the field of view of video camera 150. Thus, in step 310 the system searches the field of view of video camera 150 to determine whether it contains a human face. This step corresponds to detection step 210 described above in connection with FIG. 2.

If a face is not detected in step 310, decision step 315 fails and the system returns to step 310 to continue searching for a face in the field of view of video camera 150.

If a face is detected in step 310 (e.g., if an individual sits down to work at terminal 130 and thus enters the field of view of video camera 150), decision step 315 succeeds and the system proceeds to sub-mode two of the not-tracking mode. In sub-mode two, the system constructs a face template of the detected face. Thus, in step 325 the system extracts the detected face from the video signal provided by video camera 150. This step corresponds to alignment step 220 and normalization step 230 described above in connection with FIG. 2. After alignment and normalization have been performed, the system proceeds to step 330 where it converts the facial image into a facial representation or template as described above in connection with representation step 240 of FIG. 2.

At this point, the system enters sub-mode three of the not-tracking mode which comprises matching the acquired facial representation against the stored facial representations of individuals authorized to use computer system 100. As shown in FIG. 3, steps 335–350 comprise a loop which successively compares the acquired representation with each of the stored representations of authorized individuals until a match is found or until all of the stored representations have been examined. As noted above, the stored representations are generated from the images of authorized individuals stored in image memory 170 and are maintained in face templates memory 140.

Continuing with FIG. 3, if no match is found in steps 335–350, the systém returns to step 310 of sub-mode one. If, on the other hand, a match is found, decision step 340 succeeds and the individual in the field of view of video camera 150 is granted access to computer system 100 as indicated in step 355. In one preferred embodiment, this grant of access consists simply of enabling both the keyboard and screen of terminal 130. In a second preferred embodiment, the grant of access may be tailored to the authorization level of the individual. For example, a person with a particular authorization level might be granted access to only certain data stored in memory 120 or might be permitted to run only certain application programs.

It will be appreciated that the not-tracking mode described above provides completely passive access to computer system 100. That is, access to computer system 100 is acquired without the need to enter a password or other identifier, and with no need for a magnetic card or other "key."

Once an individual has been granted access to computer system 100, the system enters the tracking mode. In this mode, the system continuously tracks the authorized individual and continues to permit access to computer system 100 only while the individual remains within the field of view of video camera 150.

In particular, once an individual is granted access to computer system 100 in step 355 of FIG. 3, the system immediately proceeds to step 410 of FIG. 4 where it registers the authorized individual's current head position, shape, size, color and facial representation and stores this in memory 120 as a new tracking path. The data stored in the tracking path can be generated using commercially available software such as the FaceIt Developer Kit, a copy of which may be found in microfiche appendix A of this application. This tracking path is used in subsequent searches to determine whether the authorized user remains in the field of view of video camera 150.

Specifically, in step 415 the system retrieves the current head location of the authorized user from memory 120 and searches for a face in the vicinity of that location. If a face is found, the system converts the newly acquired facial image to a facial representation and compares that representation to the one stored in the tracking path. As is well known in the art, this comparison may be performed through template matching using a normalized correlator. A match is declared to exist if the normalized correlator is larger than a preset threshold value. In a preferred embodiment, computer system 100 may also compare the newly acquired representation to the facial representations stored in the face template database. As described below, when these comparisons sufficiently confirm the continued presence of the authorized individual, continued access to computer system 100 is provided.

Thus, in decision step 420, the system determines whether the acquired representation matches the facial representation stored in the tracking path. If decision step **420** succeeds, then access to computer system **100** is continued, and the system proceeds to step **425** where the information stored in the tracking path is updated in accordance with the latest acquired representation. From step **425**, the system loops back to step **415**, and a new search is begun. In this way, the identity of the authorized user is repeatedly confirmed.

At times, however, decision step **420** may fail even when the authorized individual continues to sit before terminal **130**. This may happen, for example, if the individual looks down or away from the screen of terminal **130** (and thus is not facing video camera **150**) or if his facial features are temporarily partially blocked. Therefore, as described below, when the system is unable to identify the facial features of an individual in the field of view, it proceeds to a second order identification scheme to confirm the continuing presence of the authorized individual.

Specifically, if decision step **420** fails, the system proceeds to decision step **430** where the system attempts to confirm the continuing presence of the authorized individual on the basis of other recorded features such as head location, shape, color, and size which are stored as part of the tracking path. In a preferred embodiment, step **430** may be composed of two sub-steps. In the first sub-step, the system retrieves the most recent head-location of the authorized individual from the tracking path and determines whether the field of view of video camera **150** now contains a head-shaped object in or near that location. If a head-shaped object is identified, the system proceeds to sub-step two and determines whether other features of the detected head-shaped object such as its shape, size and color, match the features stored as part of the tracking path. A score is assigned to the results of this matching process, and if the score is above a predetermined threshold, decision step **430** succeeds and access to computer system **100** is continued. In that event, the stored tracking path is updated in step **425**, and the system returns to step **415** to repeat the tracking.

Otherwise, if sub-step one fails (i.e., no head shaped object is detected) or if sub-step two fails (i.e., the matching score of the additional features is too low to indicate a match), then step **430** fails. In that event, the system disables the keyboard and screen of terminal **130**, and returns to step **310** of the not-tracking mode. In this way, the system immediately revokes access when the presence of the authorized individual ceases to be detected.

In a preferred embodiment, because identification on the basis of these additional features is less certain than facial identification, the system requires a closer spatial proximity between the detected head-shaped object and the head location stored in the tracking path than would be required to confirm a match on the basis of facial identification. This ensures the accuracy of the identification since it is impossible for an unauthorized individual to occupy the space of the authorized individual within a single cycle of the tracking mode.

It should be noted that in this preferred embodiment, the continuous monitoring cycle represented by steps **415**–**430** of the tracking mode is repeatedly executed as fast as the hardware will allow. On standard Pentium (™) hardware the time required to complete each monitoring cycle is approximately 10 to 20 milliseconds. As those skilled in the art will appreciate, when other applications in addition to the continuous monitoring program are being run on the CPU, multitasking may be employed to execute the continuous monitoring program and the other applications concurrently. In some cases, this may somewhat increase the cycle time to, for example, 30 milliseconds.

In an alternative embodiment, the tracking mode may comprise a delay step **425*a*** between step **425** and step **415**. Delay step **425*a*** causes the tracking mode to confirm the user's identity periodically rather than continuously. As will be recognized, this alternative places fewer demands on the resources of computer system **100** but provides somewhat decreased security.

In a preferred embodiment, the continuous monitoring system of the present invention may comprise an additional feature which, during tracking mode, continuously searches for additional individuals who have entered the field of view of video camera **150**. This may occur, for example, if an unauthorized individual approaches the authorized individual from behind and positions himself to read data displayed on the screen of terminal **130** over the shoulder of the authorized individual. When equipped with this feature, the tracking mode comprises an additional step **425*b*** which continuously searches for the presence of a second, unauthorized individual within reading distance of the screen of terminal **130**. When such an individual is detected, the system either disables the screen or prints a warning message to the authorized user.

In an alternative embodiment, the system employs the not-tracking mode to regulate initial access to computer system **100**, but substitutes an inactivity-detection mode for the tracking mode of the preferred embodiment to regulate continuing access to computer system **100**. In this alternative embodiment, the system interprets prolonged inactivity by the authorized user as evidence that the authorized user has left the vicinity of terminal **130**. A preferred embodiment of the inactivity-detection mode of the present invention is described in connection with FIG. **5**.

Recall that when an authorized user is recognized by the not-tracking mode, access is granted to computer system **100** (step **355** of FIG. **3**) and the not-tracking mode terminates. The system then proceeds to the inactivity-detection mode charted in FIG. **5** which employs the screen saver feature resident in most operating systems to revoke access to computer system **100** and to return the system to the not-tracking mode.

It is well known in the art that most operating systems comprise a screen saver feature. In accordance with this feature, when the operating system detects a preestablished period of user inactivity (e.g., no keyboard activity), it automatically launches a screen saver application program. Generally, the user may set the period's length and may choose the particular screen saver program to be launched. As described below, this embodiment employs a particular screen saver program written specifically to achieve the objects of the present invention.

Specifically, in step **510** of FIG. **5**, the operating system continuously monitors for a period of inactivity greater than the preestablished period. When such a period is detected, the system proceeds to step **515** wherein the operating system launches the screen saver program. The screen saver program comprises code which directs computer system **100** to disable the keyboard and screen of terminal **130** and to return the system to not-tracking mode. Accordingly, in step **520** access to computer system **100** is revoked, and the system returns to the not-tracking mode.

In this way, access is denied to computer system **100** during prolonged periods of inactivity by the authorized user. This alternative embodiment is less expensive than the preferred embodiment described above and places fewer demands on the resources of computer system **100**. It does not, however, immediately revoke access when the authorized user leaves terminal **130** and therefore provides somewhat less security than the continuous tracking of the preferred embodiment.

In a related alternative embodiment, the screen saver program directs the system to examine the field of view of video camera **150** for the presence of the authorized individual before disabling the keyboard and screen of terminal **130**. This embodiment is described in connection with FIG. **6**.

Steps **610** and **615** of this embodiment are identical to steps **510** and **515** of the embodiment charted in FIG. **5**. Thus, in steps **610** and **615**, the operating system continuously monitors the keyboard for a pre-set period of inactivity and launches the screen saver application when such a period is detected.

In step **620**, however, the screen saver program directs the system to search the field of view of video camera **150** for the face of the authorized individual initially granted access by the not-tracking mode. If the authorized individual is detected, decision step **625** succeeds, and continued access to the system is provided. Otherwise, decision step **625** fails, and the system proceeds to step **630** wherein access is revoked. From step **630**, the system returns to the not-tracking mode.

It will be appreciated that this alternative embodiment beneficially maintains continued access despite long periods of inactivity by the authorized individual as long as the authorized individual remains at terminal **130**.

In a second related alternative embodiment, the system may maintain continued access despite prolonged inactivity as long as any motion is detected in the field of view of video camera **150**. This embodiment is identical to that shown in FIG. **6**, except that in steps **620** and **625** the system searches the field of view for any movement, rather than for the presence of the authorized individual. This embodiment avoids the need for performing face recognition in steps **620** and **625** while providing continued access only when there is some indication that the authorized individual is still present.

State of the art recognition software can compare an acquired representation against up to 300 stored representations per second when run on a standard Pentium (™) processor. Therefore, when the number of authorized individuals is small, the system can quickly determine whether a particular individual is authorized.

When the number of authorized individuals is large, however, the time required to identify an individual may be substantial. Illustratively, in the present state of the art, the mean time to confirm the identity of an individual in a computer system with 25,000 authorized users is slightly over 40 seconds.

Consequently, in a further preferred embodiment, the not-tracking mode additionally comprises a speech recognition sub-mode designed to decrease the number of comparisons performed in steps **335–350** of FIG. **3**. The speech recognition sub-mode is concisely indicated as step **330***a* in FIG. **3**. A preferred embodiment of this sub-mode is more fully described in conjunction with FIG. **7**.

Recall that in step **330** of FIG. **3** the not-tracking mode creates an acquired facial representation of an individual in the field of view of video camera **150**. In this preferred embodiment, before the comparison loop represented by steps **335–350** commences, the system proceeds to step **710** wherein the individual is prompted to say his name or any other user specific phrase. In step **715**, speech recognition software is employed to detect and identify the name spoken by the individual. An example of speech recognition software suitable for this purpose is the Power Secretary by Articulate Systems.

In step **720**, the system retrieves from face template memory **140** the facial representations of all individuals whose names sound similar to the name spoken by the individual. The acquired representation is then compared only to the facial representations in this reduced universe. In this way, fast authorization determinations are possible on standard inexpensive hardware even when the universe of authorized individuals is large.

It is noted that the preferred embodiment charted in FIG. **3** employs face recognition to initially detect the presence of an individual. Speech recognition is used only to reduce the number of necessary comparisons. Alternatively, the system might instead employ speech recognition to initially detect the presence of an individual and launch the face recognition software only when an individual has been detected.

In a further preferred embodiment, the not-tracking mode may comprise a surveillance feature which stores the facial representations of unauthorized individuals who approach terminal **130** during the absence of the authorized user. When equipped with this feature, the not-tracking mode is provided with an additional step **345***a*, shown in broken lines in FIG. **3**. Recall that when decision step **345** succeeds, the system concludes that the individual in the field of view of video camera **150** is not an authorized individual. Then, in this preferred embodiment, the system proceeds to step **345***a* wherein the facial representation of the unauthorized individual is stored in a surveillance log in memory **120**. Later, when the system detects the return of the authorized individual (step **340** of FIG. **3**), it may display to the authorized individual a video image of any unauthorized individuals who approached terminal **130** during the authorized individual's absence.

In a further preferred embodiment, the system can, while in not-tracking mode, serve as a multimedia messaging center. In this embodiment, when steps **335–350** of the not-tracking mode ascertain that a face in the field of view of video camera **150** does not belong to an authorized individual, the system plays a prerecorded multimedia greeting message on terminal **130** (step **345***b*). This message may contain both a visual portion displayed on the screen of terminal **130** as well as an audio portion if terminal **130** is provided with speakers. The greeting message offers the unauthorized individual the option of leaving a multimedia message for an authorized individual. In various preferred embodiments, the message may comprise a video component (using video camera **150**), an audio component (using a microphone), a text component (using the keyboard of terminal **130**), or any combination of the above. The entered message is stored by the system (step **345***c*). Later, when the system detects the return of the authorized individual (step **340** of FIG. **3**), it informs the individual of any messages received in the individual's absence and gives the individual the option to play back the messages.

Aspects of this embodiment may be especially appropriate in securing certain physical environments, such as a family home. For example, a system embodying the not-tracking mode of the present invention in combination with the multimedia message center feature, could grant access to members of the family, while denying access to others. In addition, when a non-member of the family was recognized by the system, it could give the non-member the opportunity to leave a message for one or more of the family members.

The preferred multimedia messaging center of the present invention profits greatly from its use of face recognition.

Specifically, face recognition permits the multimedia messaging center to automatically distinguish between authorized and unauthorized individuals and to display a greeting to unauthorized individuals only. It should be recognized, however, that the multimedia messaging center of the present invention may be implemented without the use of face recognition, as well. One such embodiment is shown in FIG. **8**. This embodiment is suitable, for example, in an office environment wherein each employee is allocated a PC for his primary use.

As shown in FIG. **8**, the multimedia messaging center remains quiescent until, in step **810**, it is restored by a visitor who enters a unique keystroke pattern via the keyboard of the PC (e.g., alt-m). When thus restored, the multimedia messaging center proceeds to step **815** wherein it displays a greeting to the visitor and offers the visitor the opportunity to leave a message for the PC's primary user. In step **820**, the messaging center stores the message left by the visitor, and displays a flag on the PC's monitor indicating the existence of a message. When the user returns, he may retrieve the message.

A preferred embodiment of an enrollment program for storing the facial images of authorized users is now described. This preferred embodiment employs a software program which may be run only by a system administrator or someone with super-user privileges. The enrollment program is described in connection with FIG. **9**.

Turning to FIG. **9**, in step **905** the system administrator launches the enrollment program. In steps **910** and **915**, the system continuously searches for the face of an enrollee in the field of view of video camera **150**. Once a face is found, decision step **915** succeeds and the system proceeds to step **920** wherein the detected face is extracted from the video signal and displayed as an image on the monitor of terminal **130**. Steps **910–920** may be performed using commercially available software such as CHead::FindHeadPosition, CAlignment::FindAlignedPosition, and CFace::GetCanonicalmage of the FaceIt Developer Kit. A copy of the object code of these functions is found in microfiche Appendix A of this application.

In step **925**, the administrator is given the option of discarding this acquired image. This option is provided because it has been found that many enrollees do not wish an unflattering image of themselves to be stored in memory. If the system administrator rejects the image, then decision step **925** fails and the system returns to step **905** to search again for a face in the field of view of video camera **150**.

Otherwise, step **925** succeeds and the system proceeds to decision step **930**. There, the system determines whether the captured image is the first image acquired for the enrollee. If it is, decision step **930** succeeds and the system stores the image in image memory **170** (step **935**).

As those skilled in the art will recognize, it is possible to construct a face template from a single image of an individual. It is preferable, however, to employ two or more images in constructing the template since this yields a more refined template and commensurately more accurate face recognition.

In addition, in order to achieve a substantial refinement in the template, it is important that the plurality of images from which the template is derived be substantially dissimilar. Otherwise, the marginal information content added by each additional image is small and does not significantly improve the quality of the template. For this reason, the preferred enrollment embodiment of the present invention discards additional captured images of the enrollee unless they differ substantially from those images already stored in image memory **170**.

Specifically, returning to FIG. **9**, once an image has been stored in image memory **170** (step **935**), the system proceeds to decision step **940** wherein it is determined whether the desired number of stored images for this enrollee have been acquired. If decision step **940** succeeds, then the system has stored the desired number of images for this enrollee and the enrollment program terminates (step **945**).

Otherwise, decision step **940** fails and the system returns to steps **910–925** to acquire another acceptable image of the enrollee. The system then proceeds to decision step **930** which now fails since an image of the enrollee has already been stored in image memory **170**. The system therefore proceeds to step **950**.

The purpose of steps **950** and **955** is to ensure that the second captured image is sufficiently different from the first captured image to justify its addition to the database. Thus, in step **950**, the system converts both the second acquired image and the first acquired image into templates and compares the two. A high matching score indicates that the two images are not significantly distinct. In that event, decision step **955** succeeds and the second image is discarded. Illustratively, the threshold score required to discard an image in step **955** of FIG. **9** might be the same as the score required to identify an individual in step **340** of FIG. **3**. When decision step **955** succeeds, the system returns to step **910** to acquire another image of the enrollee.

If, however, the matching score of the comparison is low, then decision step **955** fails, and the second image is added to image memory **170**. The process is then repeated until the desired number of dissimilar images is stored in image memory **170**. Once the desired number of images have been stored, decision step **940** fails, and the enrollment program terminates.

In a preferred embodiment, the enrollment program can comprise an adaptive enrollment scheme which periodically adds an updated image of the authorized individual to image memory **170**. This preferred embodiment is described in connection with FIG. **10**.

Recall that when an authorized user is recognized by the not-tracking mode, access is granted to computer system **100** (step **355** of FIG. **3**) and the not-tracking mode terminates. In this preferred embodiment, the system then proceeds to step **1005** wherein it determines the amount of time that has passed since an image of the authorized individual was added to image memory **170**. If that amount of time exceeds a predetermined amount (which may be set by the system administrator), decision step **1010** succeeds, and the image of the authorized individual acquired in step **325** of FIG. **3** is added to image memory **170** (step **1015**). Otherwise, decision step **1010** fails, and the enrollment program terminates (step **1020**).

In this way, image memory **170** is periodically updated to reflect changes in the appearance of the authorized individual. As a result, the system can continue to recognize the authorized individual even as his appearance changes over time.

Preferably, the initial images stored at the time of enrollment are never erased, but the additional images added periodically may be replaced during subsequent periodic updates.

It should be recognized that this preferred adaptive enrollment embodiment conveniently updates the stored images of an authorized individual without requiring the individual to participate in a new enrollment procedure.

While the invention has been described in conjunction with specific embodiments, it is evident that numerous alternatives, modifications, and variations will be apparent to those skilled in the art in light of the foregoing description.

What is claimed is:

1. A method of regulating continued access to a restricted environment, comprising:

storing a facial representation of an individual authorized to have access to the restricted environment;

periodically acquiring a facial representation of an individual desiring continued access to the restricted environment;

determining repeatedly whether the individual seeking continued access is the authorized individual by comparing the most recently acquired representation to the stored representation to determine the degree to which the most recently acquired representation corresponds to the stored representation;

storing additional identifying features representative of an authorized individual;

acquiring additional identifying features of the individual desiring continued access to the restricted environment;

comparing the acquired additional features and the stored additional features when the degree of similarity between the most recently acquired facial representation and the stored facial representation does not confirm the identity of the individual seeking continued access;

revoking access to the restricted environment if the step of determining and the step of comparing indicate that the individual seeking continued access is not the authorized individual.

2. The method of claim **1** wherein the additional identifying features comprise the head location, head shape, and head size of the authorized individual.

3. The method of claim **1** wherein the stored representation is modified by at least a portion of the acquired representations.

4. The method of claim **1** further comprising:

determining if no individual is seeking access to the restricted environment; and

revoking access to the restricted environment if the determination indicates that no individual is seeking access to the restricted environment.

5. The method of claim **1** wherein the restricted environment is a physical environment.

6. The method of claim **1** wherein a video camera is employed to acquire a facial image of the individual seeking access to the restricted environment.

7. The method of claim **1** wherein the comparison is performed in real-time.

8. The method of claim **1** wherein the step of acquiring a facial representation comprises the steps of:

detecting the presence of a face in a field of view;

aligning the detected face;

normalizing the detected face; and

representing the detected face as a template.

9. The method of claim 1, further comprising:

monitoring the environment for periods of inactivity greater than a predetermined length; and

revoking access to the environment when such period of inactivity is detected.

10. The method of claim **1** further comprising a method of regulating initial access to the restricted environment, comprising:

storing facial representations of individuals authorized to have access to the restricted environment;

acquiring a representation of the face of an individual who approaches the restricted environment during a period when access to the restricted environment is impeded;

comparing the initial acquired representation to the stored representations; and

denying initial access to the restricted environment if the comparison indicates that the individual seeking initial access is not an authorized individual.

11. The method of claim **10** further comprising:

discerning the presence of a face in the field of view of a video camera.

12. The method of claim **1** wherein the restricted environment is a virtual environment.

13. The method of claim **12** wherein the virtual environment is a computer network environment.

14. The method of claim **12** wherein the virtual environment is a PC environment.

15. A method of regulating initial and continued access to a restricted environment, comprising:

storing facial representations of individuals authorized to have access to the restricted environment;

acquiring a first representation of the face of an individual who approaches the restricted environment during a period when access to the restricted environment is impeded;

comparing the first acquired representation to the stored representations;

denying initial access to the restricted environment if the comparison indicates that the individual seeking initial access is not an authorized individual and granting initial access to the restricted environment if the comparison indicates that the individual seeking initial access is an authorized individual;

acquiring a second facial representation of an individual desiring continued access to the restricted environment;

determining whether the individual seeking continued access is the authorized individual by comparing the second acquired representation to at least one of the stored representations;

revoking access to the restricted environment if the determination indicates that the individual seeking continued access is not the authorized individual;

if initial access is denied, displaying a greeting to the unauthorized individual; and

storing a message for an authorized individual from the unauthorized individual.

16. The method of claim **15** wherein the message comprises a text portion.

17. The method of claim **15** wherein the message comprises an audio portion.

18. The method of claim **15** wherein the message comprises a visual portion.

19. A method of regulating continued access to a restricted environment, comprising:

storing a facial representation of an individual authorized to have access to the restricted environment;

acquiring a facial representation of an individual desiring continued access to the restricted environment;

determining whether the individual seeking continued access is the authorized individual by comparing the acquired representation to the stored representation;

revoking access to the restricted environment if the determination indicates that the individual seeking continued access is not the authorized individual;

detecting the approach of an unauthorized second individual to the restricted environment; and

revoking access of the authorized individual to the restricted environment when the approach of the unauthorized individual is detected.

20. A method of regulating initial access to a restricted environment, comprising:

storing a plurality of facial representations of individuals authorized to have access to the restricted environment;

associating one or more words with each authorized individual;

acquiring a representation of the face of an individual who approaches the restricted environment during a period when access to the restricted environment is impeded;

recognizing the linguistic content of the one or more words when spoken by an individual seeking access to the restricted environment;

comparing the acquired representation only against the facial representations of individuals with whom the recognized one or more words are associated;

denying initial access to the restricted environment if the comparison indicates that the individual seeking initial access is not an authorized individual.

21. A continuous monitoring system for regulating access to a restricted environment, comprising:

a CPU;

a memory connected to the CPU;

a tracking path stored in the memory comprising data regarding an individual authorized to have access to the restricted environment;

the tracking path comprising at least a facial representation of the authorized individual;

a video input device connected to the CPU and having a field of view;

an image translator resident in the CPU for repeatedly receiving images in the field of view and generating therefrom data regarding an individual located in the field of view;

a comparator resident in the CPU for repeatedly comparing the generated data with the tracking path, the results of each comparison constituting a comparison result;

an access control device resident in the CPU operative in response to the comparison results;

wherein the generated data comprises a facial representation of the individual in the field of view when it is possible to acquire a facial representation of the individual;

wherein the tracking path and the generated data further comprise additional identifying data regarding the authorized individual located in the field of view; and

wherein the comparator compares the additional generated data and the additional tracking path data when it is impossible to acquire a facial representation of the individual in the field of view.

22. The system of claim 21 wherein the generated data comprises a facial representation of the individual in the field of view.

23. The system of claim 21 wherein the tracking path comprises the most current data available regarding the authorized individual.

24. The system of claim 21 wherein the access control device denies access to the restricted environment when the comparison result indicates the absence of the authorized individual.

25. The system of claim 21 wherein the image translator, comparator, and access control device operate in real-time.

26. The system of claim 21 wherein the additional data comprise the head location, head shape, and head size of the authorized individual.

27. The system of claim 26 wherein the current data is at least partially derived from the additional generated data.

28. A monitoring system for regulating continued access to a restricted environment, comprising:

means for storing a facial representation of an individual authorized to have access to the restricted environment;

means for acquiring a facial representation of an individual desiring continued access to the restricted environment;

means for repeatedly determining whether the individual seeking continued access is the authorized individual by comparing the acquired representation and the stored representation;

means for revoking access to the restricted environment if the determination indicates that the individual seeking continued access is not the authorized individual;

second means for storing additional identifying features representative of an authorized individual;

second means for acquiring additional identifying features of an individual desiring continued access to the restricted environment;

wherein the means for determining comprises a means for comparing the acquired additional features and the stored additional features when the degree of similarity between the most recently acquired facial representation and the stored facial representation does not confirm the identity of the individual seeking continued access.

29. The system of claim 28 further comprising:

means for periodically acquiring subsequent facial representations of at least one individual desiring continued access to the restricted environment;

means for repeatedly determining the degree to which the most recently acquired representation corresponds to the stored representation of the authorized individual.

30. The system of claim 28 wherein the additional identifying features comprise the head location, head shape, and head size of the authorized individual.

31. The system of claim 28 wherein the stored representation is modified by at least a portion of the acquired representations used to identify the individual desiring continued access to the restricted environment.

32. The system of claim 28 further comprising means for determining if no individual is seeking access to the restricted environment; and

means for revoking access to the restricted environment if the determination indicates that no individual is seeking access to the restricted environment.

33. The continuous video monitoring system of claim 28 wherein the restricted environment is a physical environment.

34. The system of claim 28 wherein the means for acquiring comprises a video camera.

35. The system of claim 28 wherein the means for comparing operates in real-time.

36. The system of claim 28 wherein the means for acquiring a facial representation comprises:

means for detecting the presence of a face in a field of view;

means for aligning the detected face;

means for normalizing the detected face; and

means for representing the detected face as a template.

37. The system of claim **28**, further comprising:

means for monitoring the environment for periods of inactivity greater than a predetermined length; and

means for revoking access to the environment when such period of inactivity is detected.

38. The system of claim **28** further comprising means for regulating initial access to the restricted environment, comprising:

means for storing facial representations of individuals authorized to have access to the restricted environment;

means for acquiring a representation of the face of an individual who approaches the restricted environment during a period when access to the restricted environment is impeded;

face recognition means for comparing the initial acquired representation to the stored representations; and

means for denying initial access to the restricted environment if the comparison indicates that the individual seeking initial access is not an authorized individual.

39. The system of claim **38** wherein the means for acquiring comprises:

a video input device having a field of view, and

means for discerning the presence of a face in the field of view.

40. The system of claim **28** wherein the restricted environment is a virtual environment.

41. The system of claim **40** wherein the virtual environment is a computer network environment.

42. The system of claim **41** wherein the virtual environment is a PC environment.

43. A monitoring system for regulating initial and continued access to a restricted environment, comprising:

means for storing facial representations of individuals authorized to have access to the restricted environment;

means for acquiring a first representation of the face of an individual who approaches the restricted environment during a period when access to the restricted environment is impeded;

face recognition means for comparing the first acquired representation to the stored representations;

means for denying initial access to the restricted environment if the comparison indicates that the individual seeking initial access is not an authorized individual and for granting initial access to the restricted environment if the comparison indicates that the individual seeking initial access is an authorized individual;

means for acquiring subsequent facial representations of an individual desiring continued access to the restricted environment;

means for repeatedly determining whether the individual seeking continued access is the authorized individual by comparing the subsequent acquired representations and at least one of the stored representations;

means for revoking access to the restricted environment if the means for determining determines that the individual seeking continued access is not the authorized individual;

means, operative upon detection of an unauthorized individual, for displaying a greeting to the unauthorized individual and message means for enabling the unauthorized individual to leave a message for an authorized individual.

44. The system of claim **43** wherein the message means comprises means for leaving a typewritten message.

45. The system of claim **43** wherein the message means comprises means for leaving a spoken message.

46. The system of claim **43** wherein the message means comprises means for leaving a message comprising both audio and visual components.

47. A monitoring system for regulating continued access to a restricted environment, comprising:

means for storing a facial representation of an individual authorized to have access to the restricted environment;

means for acquiring a facial representation of an individual desiring continued access to the restricted environment;

means for repeatedly determining whether the individual seeking continued access is the authorized individual by comparing the acquired representation and the stored representation;

means for revoking access to the restricted environment if the determination indicates that the individual seeking continued access is not the authorized individual;

means for detecting the approach of an unauthorized second individual to the restricted environment; and

means, triggered by detection of the unauthorized second individual, for revoking access of the authorized individual to the restricted environment.

48. A system for regulating initial access to a restricted environment, comprising:

means for storing a plurality of facial representations of individuals authorized to have access to the restricted environment;

means for associating one or more words with each authorized individual;

means for acquiring a representation of the face of an individual who approaches the restricted envioronment during a period when access to the restricted environment is impeded;

means for recognizing the linguistic content of the one or more words when spoken by an individual seeking access to the restricted environment;

means for comparing the acquired representation only against the facial representations of individuals with whom the one or more words are associated; and

means for denying intial access to the restricted environment if the comparsion indicates that the individual seeking initial access is not an authorized individual.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,111,517

DATED : August 29, 2000

INVENTOR(S) : Atick et al.

It is certified that errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

after the Title of the Invention but before the Copyright Authorization:

insert – This application contains a microfiche appendix. The microfiche appendix includes 22 microfiche and 2070 frames. –

Signed and Sealed this

Fifteenth Day of May, 2001

Attest:

Nicholas P. Godici

NICHOLAS P. GODICI

Attesting Officer

Acting Director of the United States Patent and Trademark Office

US006374145B1

(12) United States Patent
Lignoul

(10) **Patent No.: US 6,374,145 B1**
(45) **Date of Patent: Apr. 16, 2002**

(54) **PROXIMITY SENSOR FOR SCREEN SAVER AND PASSWORD DELAY**

(75) Inventor: **Mark Lignoul**, 717 Oak La., Grapevine, TX (US) 76051

(73) Assignee: **Mark Lignoul**, Grapevine, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/211,091**

(22) Filed: **Dec. 14, 1998**

(51) **Int. Cl.**^{7} **G05B 15/00**; G06F 11/30; G06F 19/00

(52) **U.S. Cl.** **700/17**; 700/83; 700/302; 703/23; 713/200; 713/203; 345/867

(58) **Field of Search** 700/17, 59, 66, 700/83, 306, 65, 84, 85, 302; 348/156, 154, 155; 713/202, 323; 703/21, 23, 24, 26; 345/158, 867; 708/135; 710/18

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,433,309 A		2/1984	Hermle et al.	331/65
4,449,122 A		5/1984	Whitmer	340/562
4,454,594 A		6/1984	Heffron et al.	713/200
4,682,159 A		7/1987	Davison	345/158
4,685,056 A		8/1987	Barnsdale, Jr. et al.	711/164
4,698,748 A		10/1987	Juzswik et al.	713/322
4,742,191 A		5/1988	Coleman et al.	200/52 R
4,825,209 A		4/1989	Sasaki et al.	340/825.72
4,886,941 A		12/1989	Davis et al.	178/19.01
5,019,804 A		5/1991	Fraden	340/562
5,059,961 A		10/1991	Cheng	345/10
5,063,306 A		11/1991	Edwards	327/77
5,270,710 A		12/1993	Gaultier et al.	341/33
5,315,884 A		5/1994	Kronberg	73/862.68
5,329,471 A	*	7/1994	Swoboda et al.	703/13
5,377,269 A		12/1994	Heptig et al.	713/202
5,380,983 A		1/1995	Cavada et al.	219/250
5,396,443 A		3/1995	Mese et al.	713/321
5,404,541 A		4/1995	Hirosawa et al.	713/324

(List continued on next page.)

OTHER PUBLICATIONS

Microsoft Press Computer Dictionary 1997, Microsoft Press, third edition, p. 272.*

Article entitled, "The Universal Serial Bus from Abstraction to Implementation", by Mohammed Fennich, Intel Corporation.

IBM Personal System/2 Mouse Technical Reference, second edition, Jun. 1989, IBM Corporation.

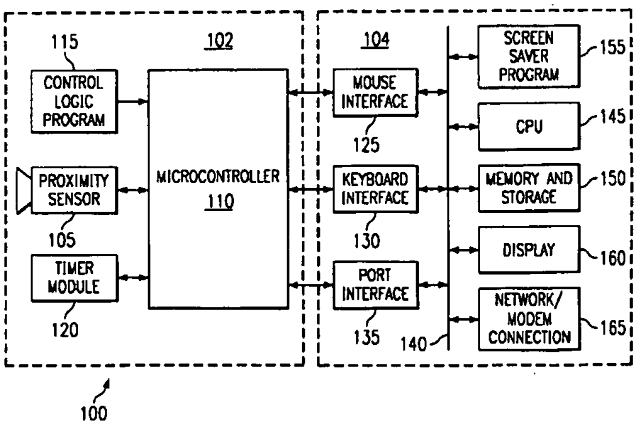
Data Handbook IC20, 80C51—Based, 8–Bit Microcontrollers, Aug. 1996, Phillips Semiconductors.

Primary Examiner—William Grant
Assistant Examiner—Paul Rodriquez
(74) *Attorney, Agent, or Firm*—J. Robert Brown, Jr.; Hunton & Williams

(57) ABSTRACT

Apparatuses and methods of the present invention provide improved control over the activation and deactivation of a computer program. For example, the computer program may be a screen saver program and/or a password protection program. The computer program is prevented from being activated when the user has not recently provided input to a computer system via an input-output device, but the user is still in the vicinity of the computer system. When no person is detected in the vicinity, the present invention allows the computer program's activation to be controlled using standard known methods. In one embodiment, the present invention provides enhanced screen saver activation and deactivation control without the need to modify existing computer hardware or software. Embodiments of modified computer hardware and software systems are also provided where it is desirable to integrate enhanced screen saver activation and deactivation control into a hardware or software system. Other aspects of the present invention deal with program activation control, user authentication, and methods for providing the most economical implementations.

20 Claims, 3 Drawing Sheets



U.S. PATENT DOCUMENTS

5,448,262	A		9/1995	Lee et al.	345/212
5,465,366	A		11/1995	Heineman	713/310
5,471,616	A	*	11/1995	Johnson et al.	713/200
5,548,763	A		8/1996	Combs et al.	713/323
5,548,764	A		8/1996	Duley et al.	713/310
5,578,991	A	*	11/1996	Scholder	340/571
5,590,315	A		12/1996	Hess et al.	703/25
5,606,615	A		2/1997	Lapointe et al.	713/185
5,640,537	A	*	6/1997	Jessen et al.	345/733
5,642,185	A		6/1997	Altrich, III et al.	399/81
5,669,004	A		9/1997	Sellers	713/324
5,675,364	A		10/1997	Stedman et al.	345/211
5,675,510	A		10/1997	Coffey et al.	709/224
5,675,810	A		10/1997	Sellers	713/323
5,682,550	A		10/1997	Brown et al.	710/10
5,689,715	A		11/1997	Crump et al.	713/310
5,715,464	A		2/1998	Crump et al.	713/323
5,736,976	A		4/1998	Cheung	345/168
5,738,527	A		4/1998	Lundberg	434/322
5,748,972	A		5/1998	Clark et al.	713/323
5,751,663	A		5/1998	Johnson	368/77
5,752,044	A		5/1998	Crump et al.	713/323
5,758,174	A		5/1998	Crump et al.	713/323
5,760,690	A		6/1998	French	340/571
5,765,001	A		6/1998	Clark et al.	359/196
5,768,602	A		6/1998	Dhuey	713/322
5,794,058	A		8/1998	Resnick	713/323
5,892,856	A	*	4/1999	Cooper et al.	382/291
5,926,404	A	*	7/1999	Zeller et al.	713/321
6,002,427	A	*	12/1999	Kipust	348/156
6,108,028	A	*	8/2000	Skarbo et al.	348/14.03
6,189,105	B1	*	2/2001	Lopes	713/202
6,282,655	B1	*	8/2001	Given	340/540
6,330,676	B1	*	12/2001	Kelsey	713/2

* cited by examiner

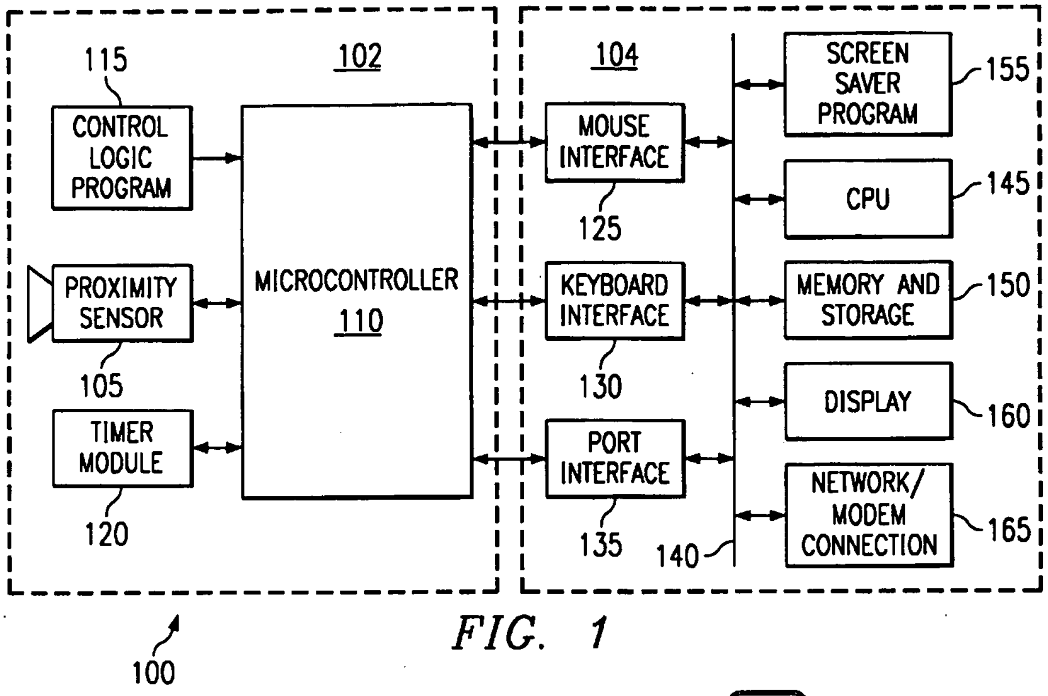

115
CONTROL LOGIC PROGRAM
102
MICROCONTROLLER 110
PROXIMITY SENSOR
105
TIMER MODULE
120
100
104
MOUSE INTERFACE
125
KEYBOARD INTERFACE
130
PORT INTERFACE
135
140
SCREEN SAVER PROGRAM
155
CPU
145
MEMORY AND STORAGE
150
DISPLAY
160
NETWORK/ MODEM CONNECTION
165

FIG. 1

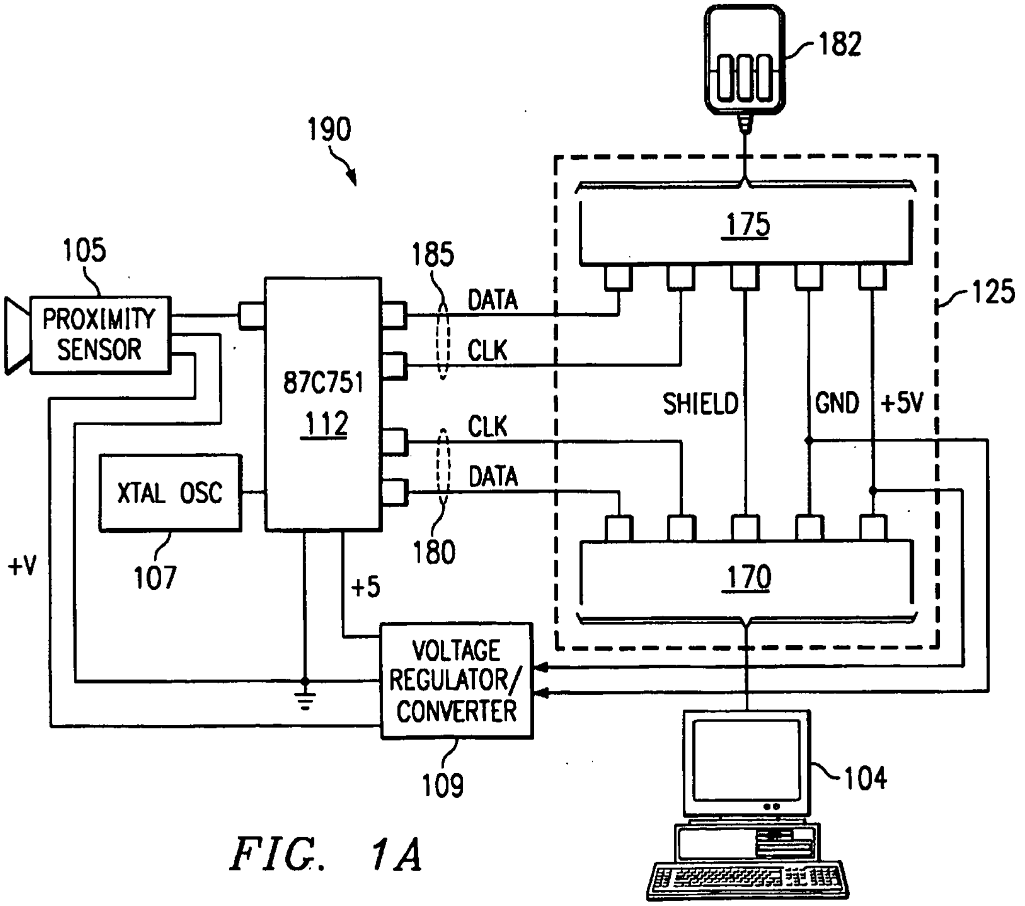

182
190
105
PROXIMITY SENSOR
185
DATA
CLK
87C751
112
CLK
DATA
180
XTAL OSC
107
+V
+5
VOLTAGE REGULATOR/ CONVERTER
109
175
125
SHIELD
GND
+5V
170
104

FIG. 1A

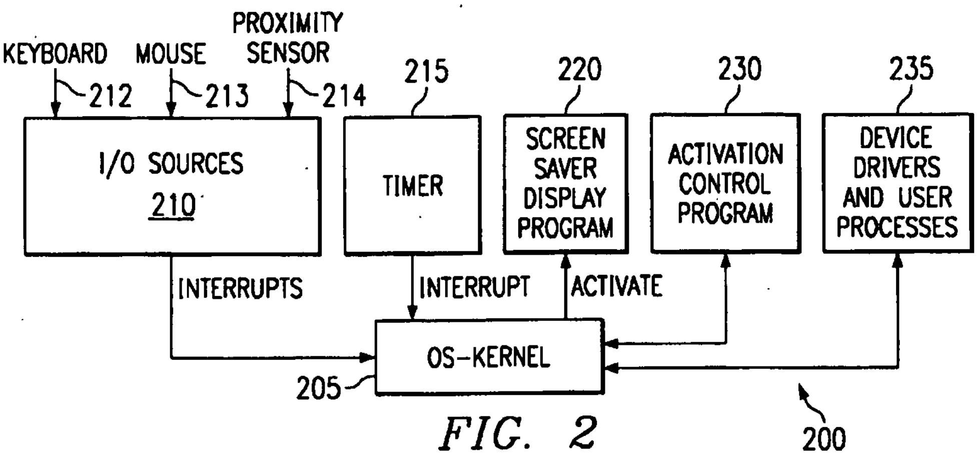


FIG. 2

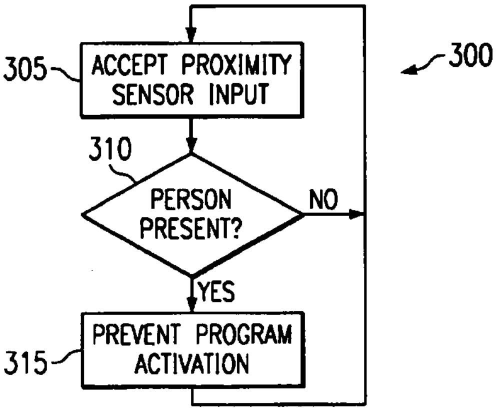


FIG. 3

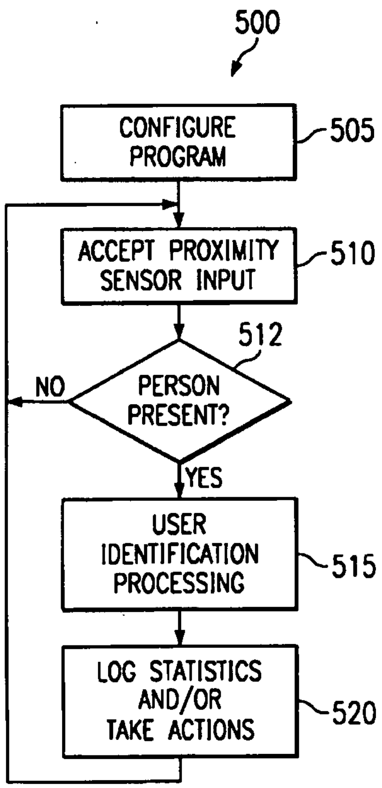

500
CONFIGURE PROGRAM
505
ACCEPT PROXIMITY SENSOR INPUT
510
512
NO
PERSON PRESENT?
YES
USER IDENTIFICATION PROCESSING
515
LOG STATISTICS AND/OR TAKE ACTIONS
520

FIG. 5

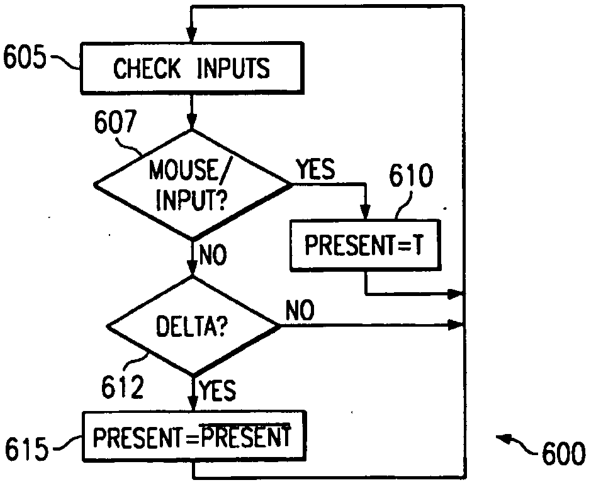


FIG. 6

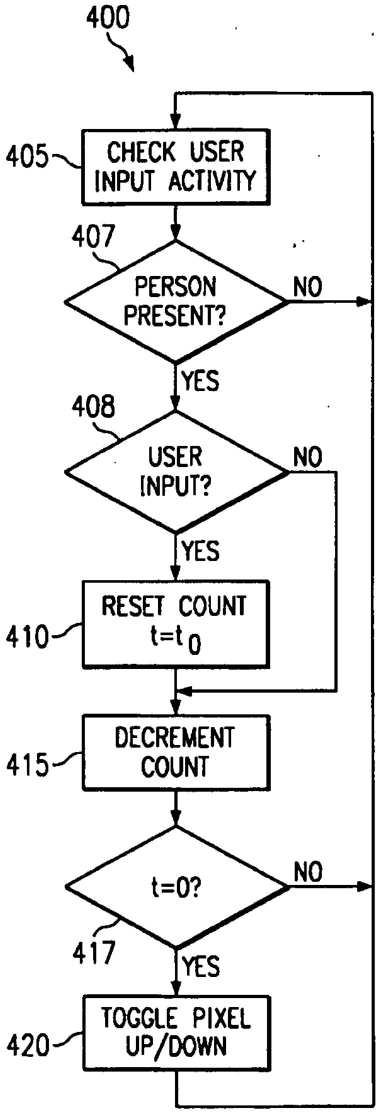

400
405
CHECK USER INPUT ACTIVITY
407
PERSON PRESENT?
NO
YES
408
USER INPUT?
NO
YES
410
RESET COUNT t=t0
415
DECREMENT COUNT
t=0?
NO
417
YES
420
TOGGLE PIXEL UP/DOWN

FIG. 4

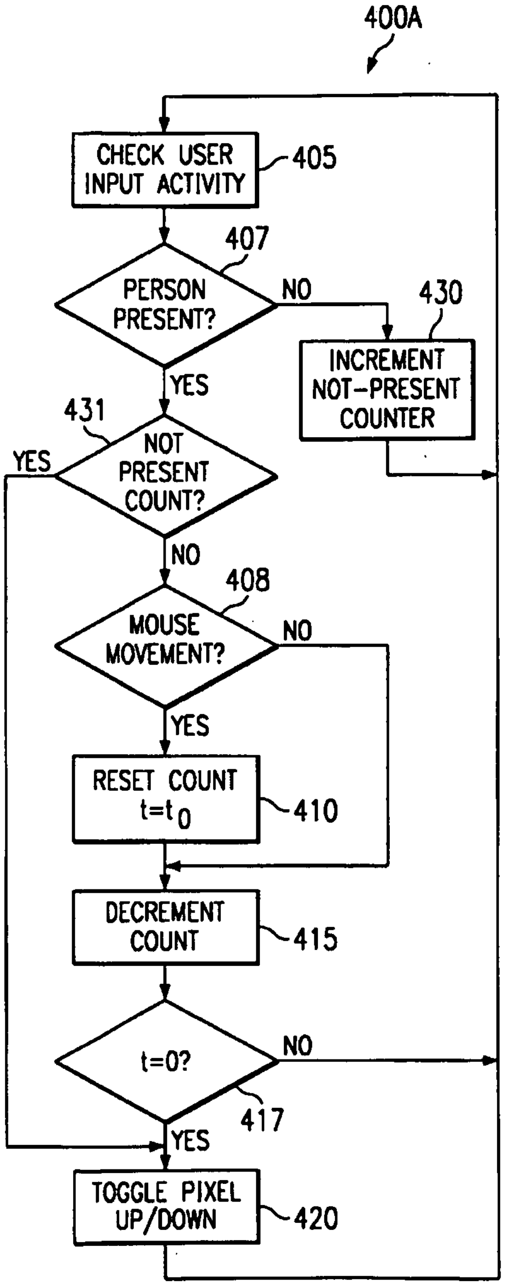

400A
CHECK USER INPUT ACTIVITY
405
407
PERSON PRESENT?
NO
430
INCREMENT NOT-PRESENT COUNTER
YES
431
NOT PRESENT COUNT?
YES
NO
408
MOUSE MOVEMENT?
NO
YES
RESET COUNT t=t0
410
DECREMENT COUNT
415
t=0?
NO
417
YES
TOGGLE PIXEL UP/DOWN
420

FIG. 4A

PROXIMITY SENSOR FOR SCREEN SAVER AND PASSWORD DELAY

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer systems. More particularly, the invention relates to a proximity sensor based control system used to prevent a computer program such as a screen saver and/or a password protection program from being activated while an operator remains present in the vicinity of a computer.

2. Description of the Related Art

Screen savers are well known in the art of computer systems. Desktop computers such as personal computers and workstations use screen savers to display an image or animation after a period of user inactivity. Likewise, laptop computers and some personal digital assistants (PDAs) also employ screen saver. technology. Screen savers are employed to prevent long-term damage which would otherwise be experienced by a computer display monitor if a single pattern such as a menu interface to an operating system were constantly displayed. Computer programs designed for use in office environments commonly display a password dialog box as a part of the screen saver image or as a stand-alone function. Password protection advantageously safeguards sensitive information held within a computer system during intermediate periods of time when the user has left the work area. Password protection with user inactivity activation allows the worker to leave the work area without needing to log out of a session with the computer. This increases security, because the user will often neglect to log out of the computer when leaving the work area to attend a meeting, eat lunch or perform other tasks away from the work area. On the other hand, the user may desire to log out of the computer session at the end of the workday.

Screen savers and password protection programs are typically activated by sensing a period of user inactivity. For example, such programs may be activated after a period of time has elapsed as measured from the last time the user has provided input to the computer using a keyboard and/or a mouse. One common method of controlling computer program activation is to use a timer. The timer is reset when an input is detected from the keyboard or the mouse. The timer is essentially a counter which counts for a predetermined number of clock cycles. After the timer has reached a predetermined count, the timer is said to "time-out." Typically, the timer generates a "time-out signal" upon time-out. The amount of time required for the timer to produce the time-out signal is called a "time-out period." Often the time-out signal is coupled to provide an interrupt to a central processing unit within the computer. When the time-out signal is detected, an interrupt request signal is provided to the central processing unit which in turn activates the screen saver and/or password protection program. Once the timer begins counting, if the user provides another input via the keyboard or the mouse, the timer is reset and begins counting anew. Thus the screen saver and/or password protection program will not be activated when the user is actively working with the computer. The screen saver and/or password protection program will only be activated after the user has remained inactive for the duration of the prespecified time-out period. The same holds true for other user activity controlled programs such as password protection programs and on-line connection programs. An on-line connection program is a program which initiates and/or deactivates a communication connection. For example, when a user has not sent any input to an on-line connection port for the duration of a time-out period, the on-line connection program will deactivate the connection so as to free up the connection port.

User activity controlled program technology as currently implemented in the art has some attendant problems. Users often become annoyed at the side effects inherent in the existing technology. For example, in the case of screen savers, while the user is actively working within his or her work area, several interruptions may occur which divert the user's attention from the computer's keyboard or mouse. In some instances the user may be involved with paperwork, a telephone call or a face-to-face interaction with a customer or colleague. In all such cases, time-out period may elapse and cause the screen saver to be activated. When the user returns to the computer desiring to interact with the operating system's user interface, the user is instead faced with a screen saver. In cases where the user needs to reenter a password, this is more than a mild annoyance. The password feature is useful in protecting the user's sensitive data when the user has left the work area for an extended period, but is more of a nuisance when the user has merely turned away to attend to another task such as a telephone call.

Hence there is a need for a user activity controlled program technology which can control the activation of a computer program without the aforementioned problems. For example, it would be desirable to have a screen saver which could provide a screen saving functionality without being activated while a user remains within the work area. It would be desirable for the computer to detect the physical presence of the user, and to use this detection to prevent a screen saver from activating. It would be desirable to include new timer algorithms adapted for use with this detection. Moreover, it would also be beneficial to provide intelligent screen saver activation control without the need to modify existing computers, screen saver software, or operating systems. It would also be desirable to integrate such a screen saver into computer hardware and software in order to provide efficient and ergonomic implementations. Systems and techniques are also needed to provide for low cost solutions as well as systems with extended functionality. Moreover, it would be desirable to have a user activity controlled program technology which could be used to activate various types of programs other than screen saver programs. Such a technology could be used, for example, to control the activation of password protection programs and online connection control programs.

SUMMARY OF THE INVENTION

The present invention solves these and other problems by providing methods and apparatus which detect the physical presence of a user and use this detection to control the activation of a user activity controlled program such as a screen saver or a password program. In a first aspect, the present invention involves an interface system which can be coupled to a computer. This system is operative to detect the physical presence of a user via a proximity sensor and to transmit a signal indicative of the presence of the user to prevent a computer program from being activated. The proximity sensor is operatively coupled to this interface system. The interface system includes a control module such as a microcontroller which causes information to be transmitted based on an output signal provided by the proximity sensor to prevent the activation of the computer program. The transmitted information is preferably embodied as a signal containing at least one bit of information designated by a logic-one voltage level, a logic-zero voltage level, or a transition therebetween. A typical value for logic-one is five volts and a typical value for logic-zero is zero volts. Typically, the transmitted information includes a sequence of bit values to form a coded command signal indicative of a mouse movement or a keyboard stroke. In one embodiment, this apparatus is supplied as an interface system which may be interposed between a computer port such as a mouse port and an input device such as a mouse. The present invention may be used to control various types of computer programs such as screen saver programs and/or password programs.

In a second aspect of the present invention, a timer is included in the interface system. When a timer is used, the interface system is operative to monitor a signal supplied by a user input-output device and monitor a signal supplied by a proximity sensor. The proximity sensor provides a signal indicative of the physical presence of a user. The system allows a computer program to be placed in a foreground state after a prespecified time duration has passed since both the user-input signal and the proximity-sensor signal have been inactive.

A third aspect of the present invention involves methods of deactivating a computer program. In a first step, the physical presence of a user is detected via a first proximity sensor. In a second step, the user is identified using at least one other proximity sensor. In a third step, a control signal is generated indicating to deactivate the computer program when the user has been identified as an authorized user. In one embodiment, the computer is a screen saver program with password protection, and in another embodiment the computer program is a stand-alone password protection program.

A fourth aspect of the present invention involves a software system for use on computers and related computerized equipment. The software system involves a background-processing module coupled to receive inputs from a user input-output device and a proximity sensor. The software system also includes a foreground-processing module which is activated in response to a control signal generated by the background-processing-module. The background-processing module maintains a timer indicative of the amount of time since a user has last applied an input via the user input-output device. The background module also accepts an input from the proximity sensor and causes the foreground-processing module to be activated. The foreground process is activated when both the timer indicates no user input has been received via the user input-output device for a prescribed amount of time and the proximity sensor indicates no user is present.

BRIEF DESCRIPTION OF THE FIGURES

The various novel features of the invention are illustrated in the figures listed below and described in the detailed description which follows.

FIG. 1 is a block diagram representing a computer system equipped with a proximity sensor and related control and interface apparatus.

FIG. 1A is a block diagram illustrating an embodiment of a proximity sensor interface which can be connected to a standard computer mouse port.

FIG. 2 is a block diagram representing a software architecture of an operating system designed to provide a proximity sensor-based input-output operations.

FIG. 3 is a flow chart illustrating a method of processing employed to provide a proximity sensor based computer program.

FIG. 4 is a flow chart illustrating a method of processing whereby a timer is employed to provide intelligent control of the activation or delay of a computer program.

FIG. 4A is a flow chart illustrating a method of processing whereby a first timer is employed to provide intelligent control of the activation of a screen saver program, and a second timer is employed to deactivate a screen saver program.

FIG. 5 is a flow chart illustrating a method of processing employed to provide enhanced services and security based on the use of a proximity sensor.

FIG. 6 is a flow chart illustrating a method of sensor signal processing used to allow a low cost proximity sensor to be used to implement a reliable overall system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In the detailed description of the preferred embodiment of the present invention which follows, specific embodiments are presented for purposes of illustration and description. While the present invention may be applied to control the activation of various types of computer programs, specific embodiments involving screen saver programs are provided herein merely by way of example. Timer controlled programs such as screen savers, password protection programs and on-line connection programs fall under the broader category of "user activity controlled programs." For example, in embodiments disclosed herein, the "screen saver" program may be substituted by or augmented with any user activity controlled program such as a password protection program or an on-line connection program. Many modifications and variations of the present invention will be apparent to those of ordinary skill in the art. Therefore, it is to be understood that the present invention encompasses all such equivalent embodiments.

FIG. 1 is a block diagram representing an embodiment of computer system **100** equipped with a proximity sensor and related control and interface apparatus. The computer system **100** includes a standard computer **104** which may be designed in accordance with the prior art. The standard computer **104** may be any workstation, personal computer, laptop computer, personal digital assistant, or other computerized apparatus which does not include or is not coupled to the proximity-sensor interface system **102**. Once the proximity-sensor interface system **102** is interfaced to the standard computer **104**, the computer system **100** results.

The proximity-sensor interface system **102** includes a proximity sensor **105** operatively coupled to a microcontroller **110**. The proximity sensor **105** may be any device which indicates the physical presence of a user. The microcontroller **110** is controllably coupled to a control logic program **115**. The combination of the microcontroller **110** and the control logic program **115** constitutes a control module. As will be discussed, the control module may be implemented using hard-coded logic and other equivalent structures. The microcontroller **110** is also coupled to a timer module **120**. In most embodiments the timer module **120** is implemented using hardware and software structures available within the microcontroller **110** itself. The microcontroller is also coupled to the standard computer **104**. In the illustrative embodiment, three interface structures are shown. The microcontroller is coupled to a computer mouse interface module **125**, a keyboard interface module **130**, and/or a port interface module **135**. In a given embodiment, one or more of these interface modules may be implemented. The interface modules **125**, **130** and **135** are preferably coupled to a user-input device. A user-input device is any device such as a mouse, a keyboard, a joystick, or a microphone which accepts inputs in response to actions of a user. The user-input device is typically designed to connect to an associated computer-input port such as a mouse port, a keyboard port, a joystick port, a microphone port, an infrared port, or a wireless interface.

The proximity sensor **105** may be implemented using various component technologies. For example, the proximity sensor **105** may be implemented using a passive infra-red sensor, a diffuse reflectance sensor, a reflectance sensor, a light beam continuity sensor, a capacitance sensor, a radio frequency (RF) sensor, an audio sensor, an ultrasonic sensor, a pressure sensitive mat, or a weight sensor within a chair. Any sensor which can detect the physical presence of a user is within the scope of the present invention.

In various systems any of these sensors may be used in combination. A sensor made up of more than one sensor is known as a multidimensional sensor since it provides a multidimensional vector of data. A multidimensional sensor made up of two or more proximity sensors is called a "multidimensional proximity sensor." For example, a multidimensional sensor may be constructed using a combination of a reflectance sensor and a RF sensor. As will be discussed in connection with FIG. **5**, the reflectance sensor allows any individual to be detected and the RF sensor allows the individual to be identified. Another example of a multidimensional sensor is a charge-coupled device (CCD) image sensor as used in a video camera. As video conferencing protocols such as the H.323 protocol from the International Telecommunications Union (ITU) become increasingly prevalent, more and more computers such as the standard computer **104** will include a CCD camera. In such cases, the existing CCD camera may be used as the proximity sensor **105** if the control logic program **115** is also employed. In a system using the existing CCD camera as the proximity sensor **105**, an image processing software program would cooperate with the control logic program **115** to recognize the presence and possibly the identity of the user. The proximity sensor **105** may also be implemented with similar technologies such as a microphone coupled to a voice recognition software program. A microphone can be used to collect a vector of speech samples and thus behaves like a multidimensional sensor. Voice recognition software analyzes a user's voice input and compares this input to a "voice print" to identify the user. Because most multimedia PCs already include microphones, solutions augmented with microphone based processing can be provided without the need for additional hardware. The embodiments making use of multidimensional sensors and signal processing techniques are discussed in connection with FIG. **5**.

The proximity sensor **105** may be physically mounted within the computer system **100** in various ways. In one embodiment, the proximity-sensor interface system **102** is built within its own enclosure as a stand-alone unit. Such an embodiment is illustrated in FIG. **1A** where the present invention is embodied as a stand-alone device which connects between the mouse **182** and the computer system **104**. Other embodiments involve building the proximity-sensor interface system **102** into a keyboard or a mouse. The computer system **104** as illustrated in FIG. **1A** includes a keyboard, a monitor and a mouse **182**. Still other embodiments involve building the proximity-sensor interface system **102** into the enclosure used to house a motherboard of the computer. This enclosure is commonly called a "CPU box" or equivalently, a "CPU tower." In FIG. **1A**, the "CPU box" is shown as being located between the keyboard and the monitor in the computer system **104**. Other embodiments may be constructed where the proximity-sensor interface system **102** is built into a computer display monitor, a mouse or a trackball, or some other add-on accessory device. The present invention comprehends all of these variations as well as other equivalent variations which may be deemed desirable as new accessories and peripherals are added to computer systems.

Various configurations may be employed to provide power to the proximity-sensor interface system **102**. Often the proximity sensor **105** will require one or more direct current (DC) voltage levels other than the ones readily available. In such cases a DC-to-DC converter may be used to transform an available voltage such as +5 volts to some other needed voltage. Other known methods are also available to derive a given voltage level from an alternating current (AC) power source.

The proximity-sensor interface system **102** controls a flow of information between the proximity sensor **105** and the standard computer **104**. In the illustrative embodiment of FIG. **1**, the flow of information is controlled using the combination of the microcontroller **110** and the control program logic **115**. In the illustrative embodiment, the control program logic **115** is implemented as a software program held within a memory module (not shown). In some embodiments, the control program logic **115** may reside in an internal memory located within the microcontroller **110**. The control program logic **115** may also reside in a static memory such as a read only memory (ROM) or an electrically erasable read only memory (EEPROM). In embodiments involving an EEPROM, the control program logic **115** may be optionally downloaded via one of the interface modules **125**, **130** and/or **135** to allow modifications to be made. In still other embodiments, the control program logic **115** may be downloaded across one of the interface modules **125**, **130**, or **135** into a volatile memory such as an SRAM chip. The microcontroller **110** may be implemented using an 87C751 from Phillips Semiconductor Inc. Other microcontrollers, such as the PIC series of microcontrollers available from Microchip, Inc., may also be used to control the flow of information between the proximity sensor **105** and the standard computer **104**. This flow of information may similarly be controlled using any available microprocessor or microcontroller.

The control module made up of the combination of the microcontroller **110** and the control logic program **115** may be alternatively implemented using one or more customized logic devices. For example a programmable logic array, a gate array or an application specific integrated circuit (ASIC) may be designed using a hard-coded state machine to control information flow and perform related logic processing. Most hard-coded logic based solutions do not require a separate memory to hold the control program logic **115** since that logic is hard-coded. The hard-coded logic based solution represents an engineering trade-off between design expenses and production expenses. When the production volume warrants, it often becomes economical to pursue the hard-coded logic based solution. In this case, the microcontroller **110** and the control program logic **115** are implemented using the hard-coded logic device. It should also be noted that some hard-coded logic devices are also reprogrammable. For example, the control program logic **115** may be downloaded via the interface module **125**, **130** or **135** into a set of volatile logic-configuration-memory cells located on a gate array as provided by Xilinx Corp. Such solutions have the advantage of being easily modified and upgraded.

The timer module **120** is preferably implemented in both hard-coded designs and microcontroller based designs using an internal programmable timer module. An internal timer includes a register to hold a count value, a counter state machine, and a coupling to a clock input. Such timer modules are well known and are available with most microcontrollers. For example, the 87C751 microcontroller from Phillips Semiconductor Inc. has an internal programmable timer module. This timer module is documented in the 87C751 microcontroller user's guide available from Phillips Semiconductor Inc.

Depending on the embodiment, one or all of the interface modules **125**, **130** and **135** may be implemented. In an exemplary embodiment, the present invention is implemented using only the mouse interface module **125**. This embodiment is discussed in detail in connection with FIG. 1A. Other embodiments use only the keyboard interface module **130**. Various types of embodiments may be constructed using the port interface module **135**. The port interface module may be implemented using a serial port such as an RS232 port, a parallel port such as a printer port, an infrared port, a wireless interface, or some specialized port such as microcontroller port interface. Similarly, a universal serial bus interface (USB) as is used to interconnect various types of computer peripherals may also be used. The port interface module **135** comprehends any custom or standardized port interface which may be used to route signals generated by the proximity-sensor interface system **102** into the standard computer **104**.

Referring again to FIG. 1, a set of component subsystems within the standard computer **104** are illustrated as being interconnected via a bus structure **140**. For example, the computer mouse interface module **125**, the keyboard interface module **130**, and the port interface module **135** are all internally coupled to the bus **140**. Also coupled to the bus **140** are a central processing unit (CPU) **145**, a memory and storage device **150**, a screen saver program **155**, a display monitor **160**, and an optional modem or network connection **165**. The screen saver program **155** preferably includes a screen saver activation control program and a screen saver display program. The screen saver activation control program monitors user inputs and activates the screen saver display program after a period of user inactivity has been detected. A mouse is generally connected to the mouse interface module **125** and a keyboard is generally connected to the keyboard interface module **130**.

In alternative embodiments, the screen saver program **155** may be any user activity controlled computer program. Also, more than one such program may be employed in a single system. For example, the screen saver program **155** of the computer system **104** may involve both a conventional screen saver program and a separate password protection program. In other embodiments, the screen saver program **155** may include a password protection feature. The discussion herein will focus on the illustrative embodiment as depicted in FIG. 1.

The bus **140** may be constructed as a set of unbroken wires or one or more optical fibers used to carry signals between the component subsystems within the standard computer **104**. In some embodiments of the present invention, the bus **140** may be implemented equivalently using a set of direct parallel and/or serial connections between individual modules. The bus **140** as illustrated in FIG. 1 shows a low cost means to connect the illustrated subsystems. A combination of bus connections and direct serial or parallel links may be used to implement a subset of the connection structure provided by the bus **140**. Different implementations represent different price-to-performance ratios and will be dictated by the needs of an individual embodiment. The bus **140** also comprehends multi-layered bus structures. For example, some embodiments make use of a local processor bus connected to the CPU **145** and the memory and storage device **150**. A peripheral interconnect bus such as a PCI bus is then used to interconnect the other subsystems. In multi-layered bus based designs, the different layers are preferably interconnected by bus bridges. All of these and other equivalent embodiments of the bus **140** are known to the skilled artisan and are considered to be equivalents of the bus **140**. From here forward, the discussion will center on the illustrated embodiment of the standard computer **104** whereby all subsystems are directly connected via the bus **140**. Embodiments where the bus **140** represents a different physical interconnection topology are implicitly included in the discussion below.

In operation, the standard computer **104** operates a screen saver program **155**. For example, whenever the user moves or clicks the mouse, information indicative of these actions are transmitted via the mouse interface module **125** to the CPU **145**. In general, the user provides an input via a user input-output device and the user input-output device transmits the information in the form of a coded-command signal made up of a sequence of voltage-levels representative of bits of the information. Typically, interrupts are generated to inform the CPU **145** when the user's input has been provided. Likewise, whenever the user applies a keystroke to the keyboard, data indicative of this activity is transmitted to the CPU **145** via the keyboard interface module **130**. The screen saver program **155** is typically resident in the memory and storage unit **150** and functions as a memory resident background process within the software structure of the computer system **100**. A timer is maintained and is updated in accordance with a timer-based interrupt. The timer is restarted with an initial count when a keyboard or mouse stroke is detected. If no keyboard or mouse input is detected for the duration of a prespecified time-out period the screen saver is moved from a background state into a foreground state. When the screen saver functions in the foreground state, it displays a static or animated pattern on the display monitor **160**. The portion of the screen saver which functions in the foreground state is also called a "screen saver display program." The portion of the screen saver program with operates in the background state is also called a "screen saver activation control program." The screen saver activation control program monitors user inputs and places the screen saver program into the foreground state after a period of user inactivity has been detected. Typically, even when the screen saver display program has been placed into the foreground state, the screen saver activation control program continues to run in the background. When a user input or physical presence is once again detected the screen saver activation control program eventually places the screen saver display program back into a background state. When the screen saver display program is in the background state it is substantially inactive.

In embodiments of the present invention involving other types of programs beside screen saver programs, the "screen saver display program" may be replaced by a more generic "operational program." For example, the activation control program **230** may control the activation of a "password protected access program." In this case, the "operational program" is the "password protected access control program." The "password protected access control program" is a program which restricts access to one or more computer programs unless a password is properly entered. Similarly, the screen saver display program may itself include a password protected access control program.

In the above discussion, the notions of a "background state" and a "foreground state" have been used. A "background-processing module" is a computer program which runs in the background state and is allowed to run concurrently with another program. Usually, the operation of a background process is transparent to the user. A "foreground-processing module" is a computer program which runs in the foreground state and whose operation is evident to the user. A foreground-processing module is typically operative to present a user interface to the user. As discussed above, the screen saver program **155** includes both a background-processing module and a foreground-processing module and can thereby operate in both the background state and the foreground state. While the user is actively using the standard computer **104**, the screen saver program **155** does not actively display a screen saver image on the display **160**. Rather, it quietly monitors the keyboard and the mouse interface activity. A counter is allowed to run and is reset every time a user input is detected. When no user inputs have been detected for a long enough time to allow the counter's time-out value to be reached, the screen saver program **155** moves into the foreground and makes its presence known by displaying the screen saver image or animation. When the screen saver moves from the background to the foreground, it is said to have been "activated." When the screen saver moves from the foreground to the background, it is said to have been "deactivated."

In accordance with the present invention, the proximity-sensor interface system **102** augments the aforementioned operation by preventing the screen saver program **155** from being activated while the user remains in the vicinity of the computer system **100**. When the proximity sensor **105** detects a user to be present, the control logic program **115** instructs the microcontroller **110** to emulate user activity by applying a data sequence to one of the interface modules **125**, **130**, or **135**. For example, in some systems the microcontroller **110** interfaces to the standard computer **104** via the mouse interface module **125**. When the proximity sensor **10** detects the user to be present, the microcontroller **110** signals the user's presence by supplying a mouse-data signal indicating to' move the cursor one or more pixels in the upward direction. A short time later, the microcontroller sends a mouse-data signal indicating to move the cursor back downward to the original position. The screen saver's counter is thus prevented from reaching its time-out value and the screen saver is prevented from activating. This added functionality is advantageously added without the need to alter the screen saver software **155** or the standard computer **104**.

In some systems, a mouse data emulation of one pixel movement is sufficient to prevent the user activity control from timing out. In other systems, depending on the screen saver activation software, an emulation of a movement of more than one pixel is required. In still other screen savers, a one pixel movement will delay the screen saver activation, but is insufficient to "wake up" the computer from a screen saver foreground state. In yet other systems, a keyboard command such as a "control" keystroke or a "function" keystroke must be emulated. The microcontroller **110** may be programmed by skilled artisans to emulate the appropriate signals needed to control the activation of screen savers and other user activity controlled programs. For example, the microcontroller **110** may be preprogrammed during manufacture to generate the proper signals to control a screen saver program. Alternatively, the microcontroller **110** may be programmed to enter a "training mode." In one embodiment of a training mode, a message is displayed asking the user to strike one or more keys to achieve a specified effect such as deactivating a screen saver. When the user strikes the one or more keys, the microcontroller **110** records associated keystroke information and subsequently uses this information to emulate user activity. Alternatively, the user may activate a switch to enter the training mode. More details regarding the operation of specific embodiments of the proximity-sensor interface system **102** are provided in connection with FIGS. **1A** to **5**.

While it is advantageous to be able to add the proximity-sensor interface system **102** to the standard computer **104** without the need to alter the design of the hardware or software of the standard computer **104**, in some cases it may be advantageous to do so. For example, when the present invention is provided as a standard feature of a computer, it is advantageous to alter the hardware and/or software of the standard computer itself. In this case instead of supplying the standard computer **104** and augmenting it with the proximity-sensor interface system **102**, the computer system **100** is manufactured and supplied as an integrated system. In such a system the screen saver activation logic which runs in the background is preferably implemented using the methods of the present invention. In this situation the proximity-sensor interface system **102** preferably makes use of the port interface module **135**, the bus **140** or other internal interface. The proximity sensor then provides input to the interrupt structure of the operating system just like the keyboard and mouse. The background-processing module within the screen saver program **155** then updates a set of variables needed to determine when to activate the screen saver program **155**. The set of variables is included in a data area which is preferably co-located along with the screen saver program **155**. The logic used to control screen saver activation in such an embodiment is described in connection with FIG. **4**. Such a modified screen saver program can be built into an operating system as discussed in connection with FIG. **2**. Before discussing these embodiments, an embodiment of the proximity-sensor interface system **102** which plugs into an existing mouse connector of the standard computer **104** is described.

Referring now to FIG. **1A**, a detailed schematic of a specific embodiment **190** of the proximity-sensor interface system **102** is illustrated. In this embodiment, only the mouse interface module **125** is used, and the microcontroller **110**, the control program logic **115** and the timer module **120** are all implemented using an 87C751 microcontroller **112**. The microcontroller **112** is coupled to receive an input from the proximity sensor **105**. An oscillator circuit **107** is also provided and is coupled to generate a clock signal for the microcontroller **112**. In this embodiment, the oscillator **107** is made up of a crystal and two capacitors which are coupled in a feedback arrangement to an amplifier located within the microcontroller **112**. This combination produces a square wave oscillator which provides a clock signal to the microcontroller **112**. In the illustrative embodiment, the mouse interface module **125** is designed using the PS/2® mouse interface protocol. An MTA41110 mouse and trackball controller IC from Microchip Inc. may be used to control this interface. The MTA41110 data sheet provides a detailed description of such an interface together with background information useful for implementing the mouse interface module **125** of the present invention. A first connector **170** is designed according to the PS/2® mouse protocol and is connectable to a mouse-port as provided by the standard computer **104**. A second connector **175** is also designed according to the PS/2® mouse protocol and is connectable to a PS/2® compatible mouse device **182**. The mouse interface module **125** is thus designed to connect between the standard computer **104** and the mouse device **182**.

The internal wiring employed within the embodiment **190** to interface the first connector **170** to the second connector **175** is illustrated in FIG. **1A**. A +5 v power wire, a ground wire, and a cable shielding wire are connected straight across the interface. The +5 volt and the ground wires are tapped off and routed to a voltage regulator **109**. The voltage regulator **109** supplies a regulated +5 volt power lead and a ground lead to the microcontroller **112** as well as any other devices needing power. In some systems the proximity sensor **105** requires DC voltage levels beside the ones shown, in which case a DC-to-DC converter may be advantageously used.

The data and clock wires do not pass straight across the interface but are rather routed to a set of input-output port pins of the 87C751 microcontroller **112**. A first pair **180** of data and clock wires are connected between first connector **170** and a first pair of input-output port pins of the microcontroller **112**. A second pair **185** of data and clock wires are connected between the second connector **175** and a second pair of input-output port pins of the microcontroller **112**. The proximity sensor **105** is also coupled to provide a digital logic input to another port pin of the microcontroller **112**. The wires carrying the data and/or the clock signals carry the "mouse-data signal" used to indicate a mouse movement. Note that a keyboard interface is very similar to a mouse interface, and embodiment **190** may be modified for the case where the data and clock wires carry keyboard-data signals indicative of keystroke activity.

In operation, the microcontroller **112** receives a set of data and clock signals from the mouse device **182** on the second pair **185** of data and clock wires. The microcontroller then echoes these received signals by transmitting them back to the standard computer **104** via the first pair **180** of data and clock wires. For example, when a user moves the mouse device **182** the data and clock wires **185** become active by carrying signal information which the microcontroller **112** will detect on its input-output port pins. The microcontroller **112** is operative to read the received data values into an internal register. Also, the microcontroller **112** echoes the data and clock signals back out the second data and clock wires **180**. This way, the standard computer **104** receives inputs sent out by the mouse device **182**. Since the microcontroller **112** passes the data signals generated by the mouse device **182** back to the standard computer **104**, the microcontroller **112** is able to monitor mouse activity. Since the microcontroller **112** is able to drive the first pair **180** of data and clock wires, it is also able to generate its own data patterns and deliver them to the standard computer **104** via the first pair **180**.

As discussed in connection with FIG. **4**, the microcontroller **112** is operative to monitor data traveling from the second pair **185** of data and clock wires **185** back to the first pair **180** of data and clock wires. When a period of inactivity is detected, and the proximity sensor detects the physical presence of the user, the microcontroller **112** is operative to insert its own data sequence and deliver it via the first pair **180** of data and lock wires back to the standard computer **104**. The data signal sent back to the standard computer **104** typically signals a mouse movement of one or more pixels in the up and/or down direction. Other movement directions such as a left and/or right may also be signaled. When this data signal is received, the screen saver background-processing module within the screen saver program **155** resets its counter as though the user had moved the mouse device **182**. In essence, the screen saver background-processing module is fooled into believing the user had moved the mouse when in fact the user was detected as being in the vicinity of the computer by the proximity sensor **105**, but no mouse movement was actually made. This allows the user to tend to other tasks such as the telephone without the screen saver being activated. In some embodiments the screen saver program **155** may include a password protection feature, and in other embodiments the screen saver program **155** may be substituted or augmented with other user activity controlled programs. More discussion relating to aspects of the operation of the proximity-sensor interface system **102** and the embodiment **190** are discussed in connection with FIG. **3–6**.

Referring now to FIG. **2**, a software architecture **200** is illustrated which can be used to control the hardware of the computer system **100**. The software architecture **200** is applicable to systems designed to accept inputs from the proximity-sensor interface system **102** via the port interface module **135**. This input is supplied to the software architecture via an input **214**. The software architecture **200** is most applicable for computers where the proximity-sensor interface system **102** is integrated into the system at the time it is manufactured as opposed to standard computers to which the proximity sensor system **102** has been added at a later time. The software architecture **200** may be supplied on a recordable medium readable by a computer system. An example of the recordable medium is a CD-ROM. The CD-ROM is inserted into a CD-ROM disc-drive, and the software with the software architecture **200** is loaded into volatile and/or non-volatile memory in the storage unit **150** of the computer system **100**. When the computer system **100** is shipped with software loaded, the software with the software architecture **200** may be already loaded into the memory and storage unit **150**.

At the center of the software architecture **200** is an operating system kernel **205**. Operating system kernels are well known in the art and control the access of software processes to the CPU **145**. A software process can be defined as a flow of instructions executed on the CPU **145**. As is common practice, the kernel **205** maintains a data structure called a task control block for each process. The kernel accepts interrupt inputs from a set of input-output sources **210** and a timer **215**. In the embodiment shown, the set of input-output sources **210** includes a keyboard **212** a mouse **213** and a proximity sensor input **214**. The kernel **205** controls the execution of multiple programs on the CPU **145** by activating and deactivating processes in response to the interrupt inputs produced by the set of input-output sources **210** and the timer **215**. An example of a process which is activated and deactivated as a function of interrupts is a screen saver display program **220**. The activation and deactivation of a set of processes **235** corresponding to device drivers and user programs are also controlled using inputs based on the interrupts supplied by the set of input-output sources **210** and the timer **215**. For example, in many operating systems, when a user moves a cursor into a window using a mouse, the program represented by the window is activated. An example of an available operating system kernel is the Unix® kernel originally developed by Bell Laboratories of AT&T, now Lucent Technologies, Inc. Other examples of operating system kernels are the kernels within the Windows98® and WindowsNT® operating systems provided by Microsoft Inc. Hence the software architecture **200** is preferably implemented as a computer operating system such as one which is shipped with the computer system **100**.

The software architecture **200** is operative to control the activation of the screen saver display program **220** by taking into account input provided by the proximity-sensor interface system **102** as supplied by the port interface module **135**. That is, a set of methods as discussed in connection with FIG. **3–5** may be practiced by an activation control program **230** which is a background-processing module and controls the activation of the screen saver display program **220**. In the software architecture **200**, an activation control program **230** is operative to analyze inputs from multiple sources to determine when to place the screen saver display program **220** into an activated foreground state whereby it displays a screen saver. That is, the software architecture **200** involves an operating system and an activation control program **230** which processes information provided via the port interface module **135**. The activation control program **230** preferably analyzes the keyboard input **212**, the mouse input **213** and the proximity sensor input **214** in determining when to activate the screen saver display program **220**.

As discussed in connection with FIG. **5**, other user activity controlled programs beside the screen saver display program **220** may be similarly activated by a program with the structure of the activation control program **230**. For example a usage statistics monitoring system may be implemented to keep statistics relating to a worker's presence in the work area, and a security system may be implemented to detect and report intruders during times where no use of the computer system **100** is authorized. These other uses are discussed in connection with FIG. **5**. In other systems, the screen saver display program **220** may be substituted by or augmented with a password protection program. In general, the screen saver display program **220** may be replaced by any operational program whose activation is controlled by the activation control program **230**.

FIG. **3** illustrates a method **300** used to control access to a computer program such as a screen saver. In a first step **305**, an input is checked based on the output of the proximity sensor **105**. Control passes out of the first step **305** based upon a decision **310**. If the proximity sensor does not detect a person to be present, no action is taken and control loops back to the first step **305**. If the proximity sensor does detect a person to be present, control passes to a second step **315**. In the step **315**, an action is taken to prevent a program such as a screen saver from being activated. As discussed in connection with FIG. **1A**, different embodiments can be used to prevent the screen saver from being activated by manipulating data sequences passed across an interface such as the mouse interface **170**. As discussed in connection with FIG. **2**, a screen saver can be prevented from being activated by analyzing the proximity sensor inputs **214** in addition to the keyboard inputs **212** and the mouse inputs **213**. The method **300** may similarly be applied to control the activation of other programs beside a screen saver.

Any program whose activation is normally governed by the detection of the absence of a keyboard or mouse input from a user may be modified in accordance with the method **300**. An example is an Internet browser or other on-line connection program. If the user does not provide any input for a time, the on-line connection program will typically disconnect the user. This causes the user to need to reconnect. Reconnecting can often be a tedious and annoying task, especially when the on-line system becomes congested and denies the user access. The method **300** can be directly applied to this type of application by detecting when the user is present in the work area and causing data to be transmitted over a communication link indicative of a keystroke or other input. As discussed in connection with FIG. **4**, a timer may be incorporated into the method **300** to allow the user to leave the work area for a specified amount of time while preventing an attached software system to time-out. For example, the user can set a variable to indicate the method **300** is to continue to prevent the on-line connection program from disconnecting for twenty minutes after the user has left the vicinity of the computer.

FIG. **4** illustrates a method **400** which corresponds to a specific embodiment of the method **300**. The method **400** is preferably implemented as a part of the control program logic **115**. The method **400** preferably runs on the microcontroller **110** and exercises the timer module **120**. The method **400** can also be implemented as a control program running on the microcontroller **112** in the specific embodiment **190**. The method **400** is operative to provide additional control to a screen saver program running on the standard computer **104**. The method **400** augments presently available screen saver activation logic with inputs provided by the proximity sensor **105**. When the user is detected by the proximity sensor **105**, the method **400** periodically transmits information to emulate a user input. In the embodiment **190**, the transmitted information indicates small mouse movements, for example one or more pixel upward and/or downward periodically at a regular thirty-second interval. The interval is controlled by the timer module **120** which uses timer-data and a counting procedure to periodically supply a time-out pulse at a prespecified interval. The net effect is to keep the screen saver from being activated without distracting the user and without needing the hardware or the software of the standard computer **104** to be modified.

In a first step **405**, a set of user inputs are sampled or otherwise recorded. The sampling of inputs represented by the first step **405** may be asynchronous. That is, the user inputs sampled in the first step **405** may be tied to interrupts and thus arrive outside of the control flow illustrated by the flowchart of the method **400**. The method **400** is itself preferably tied to a timer interrupt. In a preferred embodiment, the step **405** represents the entry point to an interrupt service routine triggered by a time-out signal generated by the timer module **120**. The timer module **120** is preferably configured to generate the time-out signal once every second. This way, the step **405** is executed once per second. Control passes from the first step **405** based on a first decision **407**. The first decision **407** is operative to pass control back to the step **405** if the proximity sensor **105** detects the user not to be present in the vicinity of the computer **100**. In the preferred embodiment, the timer module **120**'s interrupt introduces a one second delay into the control path from the first decision **407** back to the first step **405**. When this control path is taken, no inputs are provided by the method **400** and the screen saver activation program is allowed to function in its normal mode.

If the proximity sensor **105** does detect the user to be present, control passes from the first step **405** based on a second decision **408**. The second decision **408** evaluates to true if a user input has been detected. For example, in the embodiment **190**, the second decision **408** evaluates to true if a mouse movement has been detected. In other embodiments, the second decision **408** is based upon inputs from one or more other sources such as a keyboard. When the second decision **408** is affirmative, control next passes to a third step **410**. In the third step **410**, a counter variable is reset. In the embodiment **190**, this counter variable is included in a data area controlled by the method **400** and is preferably set to a value of thirty. Control next passes from the second step **410** to a third step **415**. If no user input is detected in the decision **408**, control passes directly from the first step **405** directly to the third step **415**. In the third step **415**, the counter variable is decremented. Note when user input is detected in the decision **408**, the counter is reset in the step **410** so as to inhibit the counter from decrementing to zero when a user is actively supplying inputs to the computer system **100**.

Control next passes from the third step **415** based on a third decision **417**. In the third decision **417**, the counter variable is compared to zero. If the timer variable has not decremented to zero, control passes from the third decision **417** back to the first step **405**. In the preferred embodiment, this branch incurs a one-second delay because the reentry of control into the step **405** is controlled to coincide with the timer-out signal produced by the timer module **120**. If the counter variable is detected as having counted down all the way to zero, control passes from the third step **415** to a fourth step **420**. The fourth step **420** is operative to send a signal to simulate a user input. In the illustrative embodiment **190**, the fourth step **420** is operative to send a simulated mouse command over the first pair **180** of data and clock wires to emulate a mouse movement. An internal state variable is also preferably toggled in the step **420** so the method **400** can keep track of whether to send a command to move the mouse upward and/or downward by one or more pixels. After the fourth step **420** has executed, control next passes back to the first step **405**, again with a one-second delay.

The effect of the method **400** is to send mouse movement commands and to prevent the screen saver from activating when the user is detected as being present in the vicinity of the proximity sensor **105**. In a preferred embodiment as described above, the method **400** sends a mouse-data command at a regular interval of **30** seconds to toggle the cursor position upward or downward by one or more pixels. In other preferred embodiments the cursor position may be toggled in other ways, such as, for example left and/or right by one or more pixels. When the user is actually providing user inputs, the counter variable is reset in the step **410** thereby inhibiting the transmission of additional user input signals in the step **420**. Only when the user has not provided any input for thirty seconds will a mouse movement be emulated in the step **420**.

While the method **400** is designed to operate with the screen saver activation program provided by the standard computer **104**, the method **400** also may be applied within the activation control program **230**. This alternate embodiment corresponds to the case where the computer system **100** is designed for use with the proximity-sensor interface system **102**. Typically, such embodiments involve the port interface module **135**, the bus **140**, or other internal interface. The activation control program **230** accepts the inputs provided by the input-output sources **210**. In an embodiment whereby the method **400** is implemented within the activation control program **230**, the first decision **407** is deleted and the second decision **408** checks to see if any activity has been detected on the input-output sources **210**. If the input-output sources **210** report any activity, then control passes from the first step **405** to the second step **410**. If no inputs are detected, control passes from the first step **405** to the third step **415**. This way the method **400** can be applied to screen savers and operating systems specially designed to accept control from the proximity-sensor input **214**. Moreover, while the method **400** is illustrated as controlling a screen saver display program, the method **400** may also be used to control any user activity controlled program.

A variation of the method **400**, a method **400A** is illustrated in FIG. 4A. The method **400A** augments the method **400** with the ability to automatically deactivate a user activity controlled program such as the screen saver program **155** when the user returns to the computer system **100**. For example, the user may immediately wish to check an email application for new messages. The method **400A** is most applicable when the screen saver **155** does not require the user to enter a password. As discussed in connection with FIG. **5**., the method **400A** can be also be modified to operate when the screen saver program **155** involves a password.

The method **400A**, begins with the first step **405**. As with the method **400**, this step is preferably entered once per second in coincidence with timer module **120**'s time-out signal. In the method **400A**, control passes from the step **405** under the control of the decision **407**. If the proximity sensor **105** does not detect the user to be present, the decision **407** regulates control to pass from the first step **405** to a fifth step **430**. The fifth step **430** is operative to increment a not-present counter. The not-present counter is preferably implemented as a software variable accessible by the control logic program **115** which implements the method **400A**. The not-present counter keeps track of the amount of time the user has been away from the computer **100**. If the user is gone a long time, the not-present counter preferably saturates at a maximum value to keep the counter from wrapping around to zero. In some embodiments the maximum value of the not-present counter may be as low as one.

If the first decision **407** detects a user to be present, a fourth decision **431** checks the not-present counter value to a threshold. The threshold is a number greater than or equal to one which indicates an amount of time the user has been away from the computer system **100**. If the not-present counter is greater than or equal to the threshold, then the decision **431** is operative to reset the not-present counter to zero and pass control from the step **405** directly to the step **420**. In the step **420** a pixel value is toggled as discussed in connection with the method **400**, thereby immediately deactivating the screen saver program. If the not-present counter is below the threshold, control is regulated by the decision **408** and the method **400A** proceeds identically to the method **400** as discussed above.

The effect of the foregoing sequential logic is to provide the same functionality as the method **400**, but to also deactivate the screen saver once the user has returned to the computer system **100**. The threshold value is used to filter spurious events and may be set as low as one. Setting the threshold to one is equivalent to using a single-bit state variable to indicate the user was not present in a previous pass through the method **400A** but is present in the current pass through the method. When the method **400A** or an equivalent thereof causes an input to be sent to the screen saver program **155** (or the activation control program **230**) substantially when the proximity sensor **105** detects a transition from the user not being present to the user being present.

Referring now to FIG. **5**, a method **500** is illustrated for using the input provided by the proximity-sensor interface system **102** for additional modes of control. In a first step **505** a set of program variables are set up and initialized. Control next passes to a second step **510**. All control paths into the second step **510** are preferably regulated to coincide with the time-out signal produced by the timer module **120**. For example, the second step **510** entered in response to a time-out interrupt produced by the timer module **120**. In the second step **510** inputs provided by the proximity sensor **105** are sampled. These inputs may be obtained by polling the proximity-sensor interface system **102**, or by checking a memory location written under the control of an interrupt handler. If no input is reported by the proximity sensor 105, control loops back around to the second step 510 under the control of a decision 512. This looping of control preferably incurs a delay substantially equal to the time-out period of the timer module 120. If an input is reported by the proximity sensor 105, control passes to an optional third step 515. The optional third step 515 is operative to perform a user identification process as discussed below. Control next passes from the optional third step 515 to a fourth step 520. If an input is reported by the proximity sensor 105 and the optional third step 515 is not present, control passes directly from the second step 510 to the fourth step 520. The fourth step 520 is operative to log statistics or take other actions. Examples of statistics logged or actions taken in the step 520 are presented below.

In a specific embodiment of the method 500, the fourth step 520 is operative to act as a usage statistics monitoring program which maintains a log of user activity within the work area. In a working environment, a management entity may desire to measure worker productivity based on the amount of time a worker is physically present within the proximity of the computer system 100. In another specific embodiment of the method 500, the fourth step 520 may be set up to provide an intruder alarm. For example, the worker may set an alarm-variable indicating that no user is authorized to come in the work area for a specified amount of time. Alternatively, the alarm-variable may be set based on a timer to indicate when no user is authorized to be in the work area, or could also change the required password as a function of time/day etc. When the proximity-sensor interface system 102 reports a person to be present, and the alarm-variable is set, an alarm may be sounded and a message transmitted via the network or modem connection 165. Hence the method 500 provides a means for the present invention to add features to the basic screen saver activation control as described above.

Enhanced versions of the present invention are obtained when the optional third step 515 of the method 500 is employed. The third step 515 is most useful when used with enhanced proximity sensors. As discussed in connection with FIG. 1, the proximity sensor 105 may involve a plurality of different types of sensors arranged in a parallel configuration. For example, the proximity sensor 105 may be constructed using both a passive infra-red sensor and radio frequency identification transceiver. Such a sensor employs a plurality of different proximity sensor technologies to provide a multidimensional output. A multidimensional output involves two or more output signals produced by two or more sensors. In a multidimensional sensor, the individual sensors may be of the same or different types. An example of a multidimensional sensor using substantially identical sensors is an image sensor such as a charge coupled device (CCD) camera. A CCD camera provides a set of pixel values. Together the set pixel values constitute a video image. The set of pixel values may be processed to determine the characteristics of a scene as viewed by the CDD camera. In many cases, the standard computer 104 may come equipped with a CCD camera to support video conferencing and related applications.

In a preferred embodiment of an enhanced system, the method 500 is practiced using the proximity sensor 105 which is implemented as a multidimensional proximity sensor and is constructed using both an infra-red sensor and a first radio-frequency transceiver. In this embodiment, the second step 510 is operative to check the infra-red sensor to determine if a person in present in the vicinity of the computer 100. If the infra-red sensor detects the person to be present, the decision 512 evaluates to true and control passes to the third step 515. In the third step 515, the first radio-frequency transceiver is used to authenticate the identity of the detected person. For example, a security guard or an authorized user may wear a security badge with a second radio-frequency transceiver. The third step 515 is then operative to cause an encrypted message to be transmitted from the first radio-frequency transceiver. The second radio frequency transceiver located in the security badge then deciphers the message and produces an encrypted response. In one embodiment a plurality of encrypted messages are transmitted using a set of public keys for a set of authorized users. The third step 515 next sets a user-identification variable to indicate whether the detected person has been properly authenticated as an authorized user. In some systems the user-identification variable also indicates the specific identity of the detected person. Control next passes from the third step 515 to the fourth step 520. In the fourth step 520 an action is taken based on the user-identification variable. If the detected person did not pass the authentication process of the step 515, an alarm may be sounded and a message may be transmitted via the modem or network interface 165. If the detected person was identified as a security guard, no further action is taken. If the detected person is identified to be the authorized user of the computer system 100 other actions may optionally be taken as described below. If a usage monitoring system is employed, the identity of the user may be taken into account while gathering statistics. For example, if system 100 is shared by various users, the usage statistics monitoring program may keep track of productivity of individual users.

This aforementioned authentication system may be also be preferably used to allow a user to reenter a work area without the need to reenter a password into a screen saver. In one example system, the security policy of an institution requires users log out of their computers at night, but allows screen savers with password to be used during the day. The method the method 400A is thus modified by adding authentication logic to the decision 431. If the not-present counter indicates the user was away for at least the threshold amount of time, and the user has been properly authenticated as the authorized user, then a control variable is set. When control next passes to the step 420, the step 420 analyzes the control variable, and if it is set, deactivates the screen saver. In essence, the password is supplied by the second radio frequency transceiver located in the user's badge. If proper challenge and reply protocols are used, an eves dropper cannot intercept a transmitted password. This is because a different password is needed as a reply based on the encrypted challenge transmitted by the first radio frequency transceiver. This way the only way for an unauthorized user to be able to deactivate the screen saver is to get physical possession of the user's badge. This is equivalent to the user losing control of a physical key and deemed to be an acceptable risk in most environments. The automatic screen saver deactivation feature may also be automatically disabled during certain hours of the day using computer date/time clocking and a set of parameters to configure the system 100 to implement a given security policy.

Referring now to FIG. 6, a method 600 is illustrated to preprocess the outputs of low cost sensors to provide a reliable "person-present" indication. While the method 500 and the use of multidimensional sensors support high-end systems, there is also a need to support very low cost implementations. As such, the method 600 addresses the problem of using a low cost version of the proximity sensor 105 which can only detect a delta, i.e., a change in environment. For example, a reflective proximity detector (RPD) may be employed to provide a highly reliable proximity detection, but such sensors are more costly than passive infra-red sensors. An RPD sensor includes a source of illumination such as an infra-red transmitter and then measures the reflected signal level. A passive infra-red sensor is less expensive but is only reliable at detecting a delta such as when a change in heat occurs due to a person entering or leaving the area surrounding the computer system **100**. A passive infrared sensor may be fooled especially in warm environments as the user moves about within the vicinity of the computer system **100**. Thus without suitable preprocessing, the passive infrared sensor may not be able to provide a reliable "person present" indication as used in the decisions **310**, **407** and **512**. The method **600** is designed to process an input provided by a passive infra-red sensor so as to provide a reliable and low-cost "person-present" indication.

In a first step **605**, a set of user values is sampled. The step **605** is preferably entered based on a timed interrupt such as a one-half second interrupt. In such an embodiment, the step **605** is entered every one-half second in response to a time-out signal. In some embodiments the method **600** may be incorporated into the logic of the step **305**, **405** or **510**. In such embodiments, a pass through the method **600** is allowed to run to completion before passing control from any of the steps **305**, **405** or **510**. The step **605** includes the sampling of the output of the proximity sensor **105**. In some embodiments, the sampled values are passed through a filter such as a first order infinte-impulse response filter or a finite impulse response filter designed with a low-frequency passband using well known digital filtering techniques. Filtering differential values with a low pass filter tends to smooth the set of differential input-values to provide a set non-differential values. Control passes from the step **605** based on a decision **607**. The decision **607** is affirmative if a mouse input has recently been detected. For example, the counter variable maintained in the steps **410** and **415** of the method **400** may be evaluated in the decision **607**. If the mouse has recently been used, then control passes to a step **610** which sets the person-present variable to true. This step ensures the person-present variable will be properly set at power-up time when the user first boots the machine. Preferably the counter used in the steps **410** and **415** is initialized to a large value at power-up time. Also, when a user does provide an input to the computer system **100**, the second step **610** assures the method **600** is reset into a correct and known state whereby the user is deemed to be present. Control next passes from the step **610** back to the step **605** through a delayed interrupt path. If the decision **607** detects that the no mouse input has recently been supplied, a second decision **612** is next evaluated. In the decision **612**, the proximity sensor is checked to see if a change, i.e., a delta, has been detected which is above a threshold. A threshold is used to filter out false alarms caused by the user moving around within the work area. When the delta has been detected, control passes to a step **615**. The step **615** is operative to toggle the state of the person-present variable. That is, when a large delta is detected, the state is toggled. For example, if the user has been involved in using the computer system **100**, the person present variable will be properly set upon power-up. When the person becomes inactive and leaves the work-area, the person-present variable will change state to indicate no person is present. When the person reenters the work area, the person-present variable will toggle to indicate a person is once again present. In the event the system is fooled due to adverse conditions such as warm temperatures which mask large deltas, the system will be restored to a correct state whenever a keystroke or mouse input is detected due to the logic leading into the state **610**. Hence such preprocessing allows a low-cost sensor such as a passive infrared sensor to be used to provide a reliable screen saver activation system.

In an alternative embodiment, the decision **607** checks to see whether a type of input other than a mouse input has been detected. For example, in some embodiments, the decision **607** is affirmative when a key on a keyboard has been recently used.

Although the present invention has been described with reference to a specific embodiment, other embodiments may occur to those skilled in the art without deviating from the intended scope. While many of the illustrative examples discuss embodiments using screen saver activation programs and screen saver display programs, the present invention applies to systems involving any activation program which controls the activation and/or deactivation of any computer program. Also, the method **400** does not need to be tied to a one-second interrupt but an interrupt based on any time-out period may be used. Also, the fourth step **420** of method **400** could cause a pixel movement other than the one-pixel up/down toggle. The multidimensional proximity sensor can also be configured using various combinations beside the infra-red sensor and the radio-frequency transceiver of the foregoing example. For example, a reflective proximity sensor could be used instead of the infra-red sensor. Lower cost radio frequency based sensors could be used. For example a simple low-cost transmitter could be located on the badge which transmits a given security code once per second and is inactive the rest of the time. Also, image and/or voice sensors may also be used. For example, if an image sensor is used, a face recognition module may be used to perform the user identification of the step **515** or the decision **431**. Likewise a voice recognition speaker identification system may be used to allow a user to speak a password and have the password compared to the user's unique voice print. Also additional timer and filtering logic may be added to the method **600** to further enhance the ability of the passive infra-red sensor to reliably perform in this application. Therefore, it is to be understood that the invention herein encompasses all such embodiments which do not depart from the spirit and scope of the invention as defined in the appended claims.

What is claimed is:

1. Apparatus comprising:

an interface module operatively couple able to provide input to a computer;

a proximity sensor operatively coupled to said interface, said proximity sensor operative to detect the presence of a user; and

a control module, said control module controllably coupled to said proximity sensor and said interface module, said control module having a state machine operative to cause information emulating a user input from a peripheral device of the computer to be transmitted to said computer via said interface module based on an output signal provided by said proximity sensor to prevent the activation of a computer program.

2. The apparatus according to claim **1**, wherein said computer program is a screen saver program.

3. The apparatus according to claim **1**, wherein said computer program is a password protection program.

4. The apparatus according to claim **1**, wherein said computer program is an on-line connection program.

5. The apparatus according to claim 1, further comprising a timer, said timer being coupled to said control module, wherein said control module is operative to regulate when said information is transmitted based on data provided by said timer.

6. The apparatus according to claim 5, wherein said regulation causes said information to be transmitted at regular intervals when said proximity sensor detects said user to be present.

7. The apparatus according to claim 6, further comprising:

a coupling interposed between said control module and a user input-output device, said coupling operative to carry a signal indicative of the presence of an input produced by said user input-output device;

whereby said regulation further inhibits said information from being transmitted at regular intervals when said proximity sensor detects said user to be present and said control module detects said signal.

8. The apparatus according to claim 7, wherein said information comprises a mouse-data signal.

9. The apparatus according to claim 7, wherein said information comprises a keyboard-data signal.

10. The apparatus according to claim 1, wherein said control module is further operative to cause said information to be transmitted substantially when said proximity sensor detects a transition from said user not being present to said user being present.

11. The apparatus according to claim 1, wherein said output signal of said proximity sensor indicates a delta, and said control module is further operative to preprocess said output signal using a state machine to convert said delta into a user-present signal.

12. Apparatus comprising:

an interface module interpretable between a user-input device and a computer-input port of a computer, said interface module including a first connector connectable to said user-input device and a second connector connectable to said computer-input port;

a proximity sensor operatively coupled to said interface module, said proximity sensor operative to detect the presence of a user; and

a control module, said control module controllably coupled to said proximity sensor and said interface module, said control module having a state machine operative to cause information emulating a user input from a peripheral device of the computer to be transmitted to said computer via said interface module based on an output signal provided by said proximity sensor to prevent the activation of a computer program.

13. The apparatus according to claim 12, wherein said computer program is a screen saver program.

14. The apparatus according to claim 12, wherein said computer program is a password protection program.

15. The apparatus according to claim 12, wherein said computer program is an on-line connection program.

16. The apparatus according to claim 12, wherein said user-input device is a computer-mouse device, said input port is a computer-mouse port, and said information comprises a data signal representative of a mouse movement.

17. The apparatus according to claim 12, wherein said user-input device is a computer-keyboard device, said input port is a computer-keyboard port, and said information comprises a data signal representative of a keystroke.

18. The apparatus according to claim 12, wherein said control module is further operative to pass a signal received from said first connector to said second connector and to monitor said signal to detect a user input.

19. The apparatus according to claim 18, wherein said control module further comprises a timer, and said control module is further operative to cause said information to be transmitted at regular intervals when said proximity sensor detects said user to be present.

20. The apparatus according to claim 19, wherein said control module is further operative to inhibit said information from being transmitted for a prespecified amount of time after said use input has been detected.

* * * * *